



REQUEST FOR PROPOSAL (RFP)

AMENDMENT 002 TO SOLICITATION NO. FIN-993302-2016-08-17

PLEASE REPLACE THE SOLICITATION DOCUMENT POSTED ON AUGUST 17, 2016 AND AMENDED ON AUGUST 22, 2016 WITH THE FOLLOWING.

SOME MINOR CORRECTIONS TO CLAUSES AND FORMATTING ERRORS HAS BEEN MADE.



REQUEST FOR PROPOSAL (RFP)

You are invited to submit a proposal to the individual specified below for the services detailed herein.

1. Title: IT Service Desk Software Solution and Professional Services to the Department of Finance

2. Solicitation Reference Number (#): FIN-993302-2016-08-17

3. RFP Authority

For the purposes of this RFP, the RFP Authority is:

Michelle Allen
Procurement and Contracting Officer
Department of Finance Canada
Mail and Messenger Services Unit
90 Elgin Street
Ottawa, ON K1A 0G5
Telephone: 613-369-3460
Email: Michelle.Allen@canada.ca

4. RFP Closing Date and Time

To be considered, proposals must be received by the following Closing Date and Time:

September 26, 2016 before 2 :00 p.m. Eastern Daylight Time (EDT)

Proposals received after the Closing Date and Time will be returned to the bidder(s) unopened.

5. Additional Details

- All enquiries regarding this RFP **must** be submitted in writing to the Solicitation Authority, **no less than five (5) calendar days prior to the Proposal Closing Date** to allow sufficient time for the Department of Finance to provide responses. Enquiries received after that date may not be responded to prior to the Proposal Closing Date;
- All answers that provide more information on the requirement will be posted on GETS.
- There is currently one or more Contractors performing some of the services described in this RFP.
 No Contractor is presently performing these services.



TABLE OF CONTENTS

FORMS: 3

PART 1 - GENERAL INFORMATION 4

1.1 INTRODUCTION.....4

1.2 SUMMARY4

1.3 DEBRIEFINGS.....4

PART 2 - BIDDER INSTRUCTIONS 5

2.1 STANDARD INSTRUCTIONS, CLAUSES AND CONDITIONS.....5

2.2 SUBMISSION OF BIDS.....5

2.3 ENQUIRIES - BID SOLICITATION.....5

2.4 APPLICABLE LAWS.....5

2.5 IMPROVEMENT OF REQUIREMENT DURING SOLICITATION PERIOD.....6

PART 3 - BID PREPARATION INSTRUCTIONS..... 6

3.1 BID PREPARATION INSTRUCTIONS6

3.1A - SECTION I: TECHNICAL BID6

3.1B - SECTION II: FINANCIAL BID9

3.1C - SECTION III: CERTIFICATIONS.....9

PART 4 – EVALUATION PROCEDURES AND BASIS OF SELECTION 10

4.1 EVALUATION PROCEDURES.....10

4.2 TECHNICAL EVALUATION10

4.3 FINANCIAL EVALUATION.....12

4.4 BASIS OF SELECTION.....12

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION 13

5.1 CERTIFICATIONS PRECEDENT TO CONTRACT AWARD AND ADDITIONAL INFORMATION13

PART 6 – SECURITY AND OTHER REQUIREMENTS 16

6.1 SECURITY REQUIREMENTS16

PART 7 - RESULTING CONTRACT CLAUSES 17

7.1 REQUIREMENT17

7.2 MINIMUM WORK GUARANTEE17

7.3 STANDARD CLAUSES AND CONDITIONS.....18

7.4 SECURITY REQUIREMENT.....18

7.5 CONTRACT PERIOD19

7.6 AUTHORITIES19

7.7 PROACTIVE DISCLOSURE OF CONTRACTS WITH FORMER PUBLIC SERVANTS20

7.8 PAYMENT20

7.9 INVOICING INSTRUCTIONS21

7.10 CERTIFICATIONS22

7.11 APPLICABLE LAWS.....22

7.12 PRIORITY OF DOCUMENTS22

7.13 LIMITATION OF LIABILITY - INFORMATION MANAGEMENT/INFORMATION TECHNOLOGY.....23

7.14 JOINT VENTURE CONTRACTOR24

7.15 LICENSED SOFTWARE25

7.16 LICENSED SOFTWARE MAINTENANCE AND SUPPORT25

7.17 TRAINING26



7.18 PROFESSIONAL SERVICES - GENERAL.....26

7.19 SAFEGUARDING ELECTRONIC MEDIA.....27

7.20 REPRESENTATIONS AND WARRANTIES.....28

7.21 ACCESS TO CANADA'S PROPERTY AND FACILITIES.....28

7.22 GOVERNMENT PROPERTY28

7.23 IMPLEMENTATION.....28

ANNEX "A" - STATEMENT OF WORK..... 29

ANNEX "B" - BASIS OF PAYMENT..... 33

ANNEX "C" - SECURITY REQUIREMENTS CHECK LIST..... 35

ANNEX "D" – EVALUATION CRITERIA..... 36

ANNEX "E" – FINANCIAL EVALUATION CRITERIA 42

FORMS:

- Form 1 - Bid Submission Form
- Form 2 - Substantiation of Technical Compliance Form
- Form 3 - OEM Certification Form
- Form 4 - Software Publisher Certification Form
- Form 5 - Software Publisher Authorization Form



PART 1 - GENERAL INFORMATION

1.1 Introduction

This bid solicitation is divided into seven parts plus attachments and annexes, as follows:

- Part 1 General Information: provides a general description of the requirement;
- Part 2 Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation and states that the Bidder agrees to be bound by the clauses and conditions contained in all parts of the bid solicitation;
- Part 3 Bid Preparation Instructions: provides bidders with instructions on how to prepare their bid;
- Part 4 Evaluation Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria that must be addressed in the bid, if applicable, and the basis of selection;
- Part 5 Certifications: includes the certifications to be provided;
- Part 6 Security and Other Requirements: includes specific requirements that must be addressed by bidders; and
- Part 7 Resulting Contract Clauses: includes the clauses and conditions that will apply to any resulting contract.

The Annexes include the Statement of Work the Basis of Payment, the Security Requirement, and any other annexes.

1.2 Summary

- 1.2.1 This bid solicitation is being issued to result in the award of one (1) contract from date of contract award to March 31, 2018. The professional services portion of the work must be completed by March 31, 2017. The Contractor must provide 35 licenses with associated maintenance up to March 31, 2018.
- 1.2.2 There is a security requirement associated with this requirement. For additional information, consult Part 6 – Security and Other Requirements, and Part 7 - Resulting Contract Clauses. For more information on personnel and organization security screening or security clauses, bidders should refer to the [Industrial Security Program \(ISP\)](http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html) of Public Works and Government Services Canada (<http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html>) website.
- 1.2.3 The requirement is subject to the provisions of the North American Free Trade Agreement (NAFTA), the Canada-Chile Free Trade Agreement (CCFTA), the Canada-Colombia Free Trade Agreement (CCoIFTA), the Canada-Panama Free Trade Agreement (CPanFTA) if it is in force.

1.3 Debriefings and Dispute Resolution

- 1.3.1 Debriefings: After contract award, bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the RFP Authority within 15 working days from receipt of the results of the bid solicitation process. The debriefing may be in writing, by telephone or in person.
- 1.3.2 Dispute Resolution: The Office of the Procurement Ombudsman (OPO) was established by the Government of Canada to provide an independent avenue for suppliers to raise complaints



regarding the award of contracts under \$25,000 for goods and under \$100,000 for services. You have the option of raising issues or concerns regarding the solicitation, or the award resulting from it, with OPO by contacting them by telephone at 1-866-734-5169 or by email at boa.opo@boa.opo.gc.ca. You can also obtain more information on the OPO services available to you at their website at www.opo-boa.gc.ca.

PART 2 - BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

All instructions, clauses and conditions identified in the bid solicitation by number, date and title are set out in the *Standard Acquisition Clauses and Conditions Manual* (<https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual>) issued by Public Works and Government Services Canada.

Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract.

The 2003 (2016-04-04) Standard Instructions - Goods or Services - Competitive Requirements, are incorporated by reference into and form part of the bid solicitation.

Subsection 5.4 of 2003, Standard Instructions - Goods or Services - Competitive Requirements, is amended as follows:

Delete: 60 days
Insert: 90 days

2.2 Submission of Bids

- (a) Bids must be submitted only to the Department of Finance's Mailroom by the date, time and place indicated on page 1 of the bid solicitation.
- (b) Due to the nature of the bid solicitation, bids transmitted by facsimile will not be accepted.

2.3 Enquiries - Bid Solicitation

All enquiries must be submitted in writing to the Contracting Authority no later than 5 calendar days before the bid closing date. Enquiries received after that time may not be answered.

Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as "proprietary" will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the question(s) or may request that the Bidder do so, so that the proprietary nature of the question(s) is eliminated and the enquiry can be answered to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

2.4 Applicable Laws

Any resulting contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of their bid, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of their choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the Bidders.



2.5 Improvement of Requirement During Solicitation Period

Should bidders consider that the specifications or Statement of Work contained in the bid solicitation could be improved technically or technologically, bidders are invited to make suggestions, in writing, to the Contracting Authority named in the bid solicitation. Bidders must clearly outline the suggested improvement as well as the reasons for the suggestion. Suggestions that do not restrict the level of competition nor favour a particular bidder will be given consideration provided they are submitted to the Contracting Authority in accordance with the article entitled "Enquiries - Bid Solicitation". Canada will have the right to accept or reject any or all suggestions.

PART 3 - BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

Canada requests that Bidders provide their bid in separately bound sections as follows:

- Section I: Technical Bid (1 hard copy and 1 electronic copy)
- Section II: Financial Bid (1 hard copy and 1 electronic copy)
- Section III: Certifications (1 hard copy and 1 electronic copy)

If there is a discrepancy between the wording of the soft copy and the hard copy, the wording of the hard copy will have priority over the wording of the soft copy.

Prices must appear in the financial bid only. No prices must be indicated in any other section of the bid.

Canada requests that Bidders follow the format instructions described below in the preparation of their bid:

- (a) use 8.5 x 11 inch (216 mm x 279 mm) paper;
- (b) use a numbering system that corresponds to the bid solicitation.

In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process [Policy on Green Procurement](http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html) (<http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html>). To assist Canada in reaching its objectives, Bidders should:

- 1) use 8.5 x 11 inch (216 mm x 279 mm) paper containing fibre certified as originating from a sustainably-managed forest and containing minimum 30% recycled content; and
- 2) use an environmentally-preferable format including black and white printing instead of colour printing, printing double sided/duplex, using staples or clips instead of cerlox, duotangs or binders.

Section I: Technical Bid

In their technical bid, Bidders should demonstrate their understanding of the requirements contained in the bid solicitation and explain how they will meet these requirements. Bidders should demonstrate their capability in a thorough, concise and clear manner for carrying out the work.



The technical bid should address clearly and in sufficient depth the points that are subject to the evaluation criteria against which the bid will be evaluated. Simply repeating the statement contained in the bid solicitation is not sufficient. In order to facilitate the evaluation of the bid, Canada requests that Bidders address and present topics in the order of the evaluation criteria under the same headings. To avoid duplication, Bidders may refer to different sections of their bids by identifying the specific paragraph and page number where the subject topic has already been addressed.

The technical bid consists of the following:

- a) **Bid Submission Form:** Unless specified otherwise in the RFP, Bidders are requested to include the completed Bid Submission Form with their bids. It provides a common form in which bidders can provide information required for evaluation and contract award, such as a contact name, the Bidder's Procurement Business Number, the Bidder's status under the Federal Contractors Program for Employment Equity, etc. Using the form to provide this information is not mandatory, but it is recommended. If Canada determines that the information required by the Bid Submission Form is incomplete or requires correction, Canada will provide the Bidder with an opportunity to do so.
- b) **Security and Other Requirements:** As required by Part 6 of the bid solicitation.
- c) **Substantiation of Technical Compliance Form:** The technical bid must substantiate the compliance of the Bidder and its proposed [solution and products] with the specific articles of Annex A (Statement of Work) identified in the Substantiation of Technical Compliance Form, which is the requested format for providing the substantiation. The Substantiation of Technical Compliance Form is not required to address any parts of this bid solicitation not referenced in the form. The substantiation must not simply be a repetition of the requirement(s), but must explain and demonstrate how the Bidder will meet the requirements and carry out the required Work. Simply stating that the Bidder or its proposed solution or product complies is not sufficient. Where Canada determines that the substantiation is not complete, the Bidder will be considered non-responsive and disqualified. The substantiation may refer to additional documentation submitted with the bid - this information can be referenced in the "Reference" column of the Substantiation of Technical Compliance Form, where bidders are requested to indicate where in the bid the reference material can be found, including the title of the document, and the page and paragraph numbers; where the reference is not sufficiently precise, Canada may request that the Bidder direct Canada to the appropriate location in the documentation.
- d) **Previous Similar Projects:** Where the bid must include a description of previous similar projects:
 - (i) a project must have been completed by the Bidder itself (and cannot include the experience of any proposed subcontractor or any affiliate of the Bidder);
 - (ii) a project must have been completed by the bid closing date;
 - (iii) each project description should include, the name, telephone number and e-mail address of a customer reference;
 - (iv) if more similar projects are provided than requested, Canada will decide in its discretion which projects will be evaluated. A project will be considered "similar" to the Work to be performed under any resulting contract if the project was for the performance of work that closely matches requirements defined in **Attachment Annex A – Statement of Work**.
- e) **Résumés for Proposed Resources:** Unless specified otherwise in the RFP, the technical bid must include résumés for the resources identified in the bid solicitation that demonstrate that each proposed individual meets the qualification requirements described (including any educational requirements, work experience requirements, and professional designation or membership requirements). With respect to résumés and resources:
 - (i) Proposed resources may be employees of the Bidder or employees of a subcontractor, or these individuals may be independent contractors to whom the Bidder would subcontract a



portion of the Work. (refer to Part 5, Certifications). For educational requirements for a particular degree, designation or certificate, the Contracting Authority will only consider educational programmes that were successfully completed by the resource by the time of bid closing.

- (ii) For requirements relating to professional designation or membership, the resource must have the required designation or membership by the time of bid closing and must continue, where applicable, to be a member in good standing of the profession's governing body throughout the evaluation and Contract Period.
- (iii) For work experience, the Contracting Authority will not consider experience gained as part of an educational programme, except for experience gained through a formal co-operative programme at a post-secondary institution.
- (iv) For any requirements that specify a particular time period (e.g., 2 years) of work experience, the Contract Authority will disregard any information about experience if the individual's résumé does not include the relevant dates for the experience claimed (i.e., the start date and end date).
- (v) For work experience to be considered by the Contracting Authority the résumé must not simply indicate the title of the individual's position, but must demonstrate that the resource has the required work experience by explaining the responsibilities and work performed by the individual while in that position. The Bidder should provide complete details as to where, when, month and year, and how, through which activities/responsibilities, the stated qualifications/experience were obtained. In situations in which a proposed resource worked at the same time on more than one project, only one project will be counted toward any requirements that relate to the individual's length of experience.
- (vi) **Implementation Plan:** The Bidder must include a proposed draft implementation plan, which demonstrates that the Bidder's proposed implementation plan meets all the mandatory requirements for implementation described in this RFP.
- (vii) **Description of the Bidder's Maintenance and Support Services:** The Bidder must include a description of its maintenance and support services for software, which must be consistent with all the requirements described in the Resulting Contract Clauses, including the Statement of Work. At a minimum, the Bidder must describe its:
 - Problem reporting and response procedures;
 - Escalation procedures;
 - On-site support availability; and
 - Any enhancements to the basic requirements that the Bidder is offering.

The Bidder may also describe any other information it considers relevant.

- (viii) **Customer Reference Contact Information:** The Bidder must provide customer references who must confirm, when requested by Canada, the facts identified in the Bidder's proposal. For each customer reference, the Bidder must, at a minimum, provide the name and either the telephone number or e-mail address for a contact person. Bidders are also requested to include the title of the contact person. If the named individual is unavailable when required during the evaluation period, the Bidder may provide the name and contact information of an alternate contact from the same customer.
- (ix) **List of Proposed Software:** The Bidder must include a complete list identifying both the name and the version number of each component of the Licensed Software required for the proposed Software Solution.



- (x) **Solution System Architecture:** The Bidder must include an overview of the proposed Software Solution's technical architecture.
- (xi) **Description of Evolution of Software Solution:** The Bidder is requested to describe when and how the proposed Software Solution was conceived and how it has evolved, with the accomplishments of each release. This is requested for information purposes only and will not be evaluated.

3.1B - Section II: Financial Bid

Bidders must submit their financial bid in accordance with the Pricing Table detailed in **Attachment Annex B - Basis of Payment**.

- a) **Pricing:** The total amount of Goods and Services Tax or Harmonized Sales Tax must be shown separately, if applicable. Prices must be firm prices.
- b) **All Costs to be Included:** The financial bid must include all costs for the requirement described in the bid solicitation for the entire Contract Period, including any option years. The identification of all necessary equipment, software, peripherals, cabling and components required to meet the requirements of the bid solicitation and the associated costs of these items is the sole responsibility of the Bidder.
- c) **Blank Prices:** Bidders are requested to insert "\$0.00" for any item for which it does not intend to charge or for items that are already included in other prices set out in the tables. If the Bidder leaves any price blank, Canada will treat the price as "\$0.00" for evaluation purposes and may request that the Bidder confirm that the price is, in fact, \$0.00. No bidder will be permitted to add or change a price as part of this confirmation. Any bidder who does not confirm that the price for a blank item is \$0.00 will be declared non-responsive.
- d) **Exchange Rate Fluctuation**

[C3011T \(2013-11-06\)](#), Exchange Rate Fluctuation

3.1C - Section III: Certifications

Bidders must submit the certifications and additional information required under Part 5.



PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

4.1 Evaluation Procedures

- (a) Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical and financial evaluation criteria. There are several steps in the evaluation process, which are described below. Even though the evaluation and selection will be conducted in steps, the fact that Canada has proceeded to a later step does not mean that Canada has conclusively determined that the Bidder has successfully passed all the previous steps. Canada may conduct steps of the evaluation in parallel.
- (b) An evaluation team composed of representatives of Canada will evaluate the bids.
- (c) In addition to any other time periods established in the bid solicitation:
 - (i) **Requests for Clarifications:** If Canada seeks clarification or verification from the Bidder about its bid, the Bidder will have 2 working days (or a longer period if specified in writing by the Contracting Authority) to provide the necessary information to Canada. Failure to meet this deadline will result in the bid being declared non-responsive.
 - (ii) **Requests for Interviews:** If Canada wishes to interview the Bidder and/or any or all of the resources proposed by the Bidder to fulfill the requirements of the bid solicitation, the Bidder will have 2 working days (or a longer period if specified in writing by the Contracting Authority) following notice by the Contracting Authority to make any necessary arrangements (at the Bidder's sole cost) for the interview to take place at a location specified by Canada.
 - (iii) **Extension of Time:** If additional time is required by the Bidder, the Contracting Authority may grant an extension in his or her sole discretion.

4.2 Technical Evaluation

- (a) **Mandatory Technical Criteria:** Each bid will be reviewed for compliance with the mandatory requirements of the bid solicitation. All elements of the bid solicitation that are mandatory requirements are identified specifically with the words "must" or "mandatory". Bids that do not comply with each and every mandatory requirement will be considered non-responsive and be disqualified.

Claims in a bid that a future upgrade or release of any of product included in the bid will meet the mandatory requirements of the bid solicitation, where the upgrade or release is not available at bid closing, will not be considered.
- (b) Mandatory technical evaluation criteria are included in Annex D: Evaluation Criteria.
- (c) **Resource Qualifications:** The qualifications and experience of the proposed resource(s) will be assessed against the requirements set out in the bid solicitation. Canada may request proof of successful completion of formal training, as well as reference information. The Contracting Authority reserves the right to request references from a Bidder to conduct a reference check to verify the accuracy of the information provided. For each customer reference, the Bidder should provide the name, telephone number and e-mail address (unless this individual does not have an e-mail address) for a contact person. The title of each person is requested but not required. If the named individual is unavailable when required during the evaluation period, the Bidder may provide the name and contact information of an alternate contact from the same customer.
- (d) **Reference Checks:** If reference checks are conducted by Canada, they will be conducted in writing by e-mail (unless the contact at the reference is only available by telephone). Canada will send all e-mail reference check requests to contacts supplied by all the Bidders on the same day. Canada will not award any points unless the response is received within 5 working days. Wherever information provided by a reference differs from the information supplied by the Bidder, the information supplied by the reference will be the information evaluated. Points will only be



allocated if the reference customer is an outside client of the Bidder itself and not that of an affiliate (for example, the outside client cannot be the customer of an affiliate of the Bidder.) Points will not be allocated if the outside client is itself an affiliate or other entity that does not deal at arm's length with the Bidder. Crown references will be accepted.

(e) **Consideration of Additional Software Use Terms included in Top-Ranked Bid:**

- (i) Acceptance of all the terms and conditions contained in Part 7 - Resulting Contract Clauses (including those relating to software licensing and those incorporated by reference) is a mandatory requirement of this bid solicitation.
- (ii) However, Bidders may, as part of their bid, submit additional software use terms. Whether or not those software use terms will be included in any resulting contract (as an Annex in accordance with the Article entitled "Priority of Documents" in the Resulting Contract Clauses) will be determined using the process described below. Whether or not any proposed additional software use terms are acceptable to Canada is a matter solely within the discretion of Canada.
- (iii) The process is as follows:
 - (A) Bids may include additional software use terms that are proposed to supplement the terms of the Resulting Contract Clauses. Bidders should not submit a software publisher's full standard license terms (because full standard license terms generally contain provisions that deal with more than simply how the software can be used; for example, they frequently deal with issues such as limitation of liability or warranty, neither of which are software use terms);
 - (B) In cases where the Bidder has submitted a software publisher's full standard license terms, Canada will require that the Bidder remove these terms and submit only the software use terms that the Bidder would like Canada to consider;
 - (C) Canada will review the additional software use terms proposed by the top-ranked Bidder (identified after the financial evaluation) to determine if there are any provisions proposed by the Bidder that are unacceptable to Canada;
 - (D) If Canada determines that any proposed software use term is unacceptable to Canada, Canada will notify the Bidder, in writing, and will provide the Bidder with an opportunity to remove that provision from its bid or to propose alternate language for consideration by Canada. Canada may set a time limit for the Bidder to respond; if the Bidder submits alternate language, if Canada does not find the alternate language acceptable, Canada is not required to allow the Bidder to submit further alternate language;
 - (E) If the Bidder refuses to remove provisions unacceptable to Canada from its bid within the time limit set by Canada in its notice, the bid will be considered non-responsive and be disqualified; Canada may then proceed to the next-ranked bid; and
 - (F) If the Bidder agrees to remove the provisions that are unacceptable to Canada and it is awarded any resulting contract, the proposed additional software use terms (as revised) will be incorporated as an annex to the contract, as set out in the Article entitled "Priority of Documents" in the Resulting Contract Clauses.

For greater certainty and to ensure that only additional software use terms that have been approved by both parties are incorporated into any resulting contract, unless the additional software use terms proposed by the Bidder are included as a separate annex to the Contract and initialed by both parties, they will not be considered part of any resulting contract (even if they are part of the bid that is incorporated by reference into the resulting contract). The fact that some additional terms and conditions or software use terms were included in the bid will not result in those terms applying to any resulting contract, regardless of whether or not Canada has objected to them under the procedures described above.



4.3 Financial Evaluation

Unless otherwise specified in the RFP, the financial evaluation will be conducted by calculating the Total Bid Price using the Pricing Table in **Annex E: Financial Evaluation Criteria**, completed by the bidders. The Bidder must provide firm, all inclusive, prices for the solution. Price will be evaluated in Canadian Dollars.

4.3.1 Mandatory Financial Criteria

Formulae in Pricing Table: If the pricing tables provided to bidders include any formulae, Canada may re-input the prices provided by bidders into a fresh table, if Canada believes that the formulae may no longer be functioning properly in the version submitted by a bidder.

4.4 Basis of Selection

A bid must comply with the requirements of the Request for Proposal and meet all mandatory technical evaluation criteria to be declared responsive. The responsive bid with the lowest evaluated price will be recommended for contract award.

4.4.1

- a) A bid must comply with the requirements of the bid solicitation and meet all mandatory criteria to be declared responsive.
- b) Bidders should note that all contract awards are subject to Canada's internal approvals process, which includes a requirement to approve funding in the amount of any proposed contract. Despite the fact that the Bidder may have been recommended for contract award, a contract will only be awarded if internal approval is granted according to Canada's internal policies. If approval is not granted, no contract will be awarded.
- c) Notification of Evaluation Results:
- d) All Bidders who respond to this RFP will be notified in writing regarding the outcome of the RFP process. This notice will include the following information:
 - 1) Solicitation Number;
 - 2) Company name of winning bidder including total points scored;
 - 3) Total value of contract awarded;
 - 4) Number of responses received by the Contracting Authority; and
 - 5) Total points scored of the Bidder (Note: Bidders will only receive their own total points scored and not the score of the other bidders)



PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

Bidders must provide the required certifications and additional information to be awarded a contract. Canada will declare a bid non-responsive if the required certifications are not completed and submitted in accordance with the articles below.

The certifications provided by Bidders to Canada are subject to verification by Canada at all times. Canada will declare a bid non-responsive, or will declare a contractor in default if any certification made by the Bidder is found to be untrue, whether made knowingly or unknowingly, during the bid evaluation period or during the contract period.

The Contracting Authority will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply and to cooperate with any request or requirement imposed by the Contracting Authority will render the bid non-responsive or constitute a default under the Contract.

5.1 Certifications Precedent to Contract Award and Additional Information

The certifications and additional information listed below should be submitted with the bid but may be submitted afterwards. If any of these required certifications or additional information is not completed and submitted as requested, the Contracting Authority will inform the Bidder of a time frame within which to provide the information. Failure to provide the certifications or the additional information listed below within the time frame specified will render the bid non-responsive.

5.1.1 Certification

(a) Contracts awarded to former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny, and reflect fairness in the spending of public funds. In order to comply with Treasury Board policies and directives on contracts awarded to FPS, bidders must provide the information required below before contract award. If the answer to the questions and, as applicable the information required have not been received by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to comply with Canada's request and meet the requirement within the prescribed time frame will render the bid non-responsive.

(b) Definitions

For the purposes of this clause, "former public servant" is any former member of a department as defined in the *Financial Administration Act*, R.S., 1985, c. F-11, a former member of the Canadian Armed Forces or a former member of the Royal Canadian Mounted Police. A former public servant may be:

- (i) an individual;
- (ii) an individual who has incorporated;
- (iii) a partnership made of former public servants; or
- (iv) a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"lump sum payment period" means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the size of the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

"pension" means a pension or annual allowance paid under the *Public Service Superannuation Act* (PSSA), R.S., 1985, c.P-36, and any increases paid pursuant to the *Supplementary Retirement Benefits Act*, R.S., 1985, c.S-24 as it affects the PSSA. It does not include pensions



payable pursuant to the Canadian Forces Superannuation Act, R.S., 1985, c.C-17, the Defence Services Pension Continuation Act, 1970, c.D-3, the Royal Canadian Mounted Police Pension Continuation Act, 1970, c.R-10, and the Royal Canadian Mounted Police Superannuation Act, R.S., 1985, c.R-11, the Members of Parliament Retiring Allowances Act, R.S., 1985, c.M-5, and that portion of pension payable to the Canada Pension Plan Act, R.S., 1985, .C-8.

(c) **Former Public Servant in Receipt of a Pension**

As per the above definitions, is the Bidder a FPS in receipt of a pension? **Yes () No ()**

If so, the Bidder must provide the following information, for all FPS in receipt of a pension, as applicable:

- (i) name of former public servant;
- (ii) date of termination of employment or retirement from the Public Service.

By providing this information, Bidders agree that the successful Bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with Contracting Policy Notice: 2012-2 and the Guidelines on the Proactive Disclosure of Contracts.

(d) **Work Force Adjustment Directive**

Is the Bidder a FPS who received a lump sum payment pursuant to the terms of the Work Force Adjustment Directive? **Yes () No ()**

If so, the Bidder must provide the following information:

- (i) name of former public servant;
- (ii) conditions of the lump sum payment incentive;
- (iii) date of termination of employment;
- (iv) amount of lump sum payment;
- (v) rate of pay on which lump sum payment is based;
- (vi) period of lump sum payment including start date, end date and number of weeks;
- (vii) number and amount (professional fees) of other contracts subject to the restrictions of a work force adjustment program.

For all contracts awarded during the lump sum payment period, the total amount of fees that may be paid to a FPS who received a lump sum payment is \$5,000, including Applicable Taxes.

5.1.2 Professional Services Resources

- (a) By submitting a bid, the Bidder certifies that, if it is awarded a contract as a result of the bid solicitation, every individual proposed in its bid will be available to perform the Work as required by Canada's representatives and at the time specified in the bid solicitation or agreed to with Canada's representatives.
- (b) By submitting a bid, the Bidder certifies that all the information provided in the résumés and supporting material submitted with its bid, particularly the information pertaining to education, achievements, experience and work history, has been verified by the Bidder to be true and accurate. Furthermore, the Bidder warrants that every individual proposed by the Bidder for the requirement is capable of performing the Work described in the resulting contract.
- (c) If the Bidder is unable to provide the services of an individual named in its bid due to the death, sickness, extended leave (including parental leave or disability leave), retirement, resignation or



dismissal for cause of that individual, within five business days of Canada's knowledge of the unavailability of the individual the Bidder may propose a substitute to the Contracting Authority, providing:

- (i) the reason for the substitution with substantiating documentation acceptable to the Contracting Authority;
- (ii) the name, qualifications and experience of a proposed replacement immediately available for work; and
- (iii) proof that the proposed replacement has the required security clearance granted by Canada, if applicable.

No more than one substitute will be considered for any given individual proposed in the bid. In response to the Bidder's proposed substitution, the Contracting Authority may elect in its sole discretion either to:

- (iv) set aside the bid and give it no further consideration; or
- (v) evaluate the replacement in accordance with the requirements of the bid solicitation in the place of the original resource as if that replacement had originally been proposed in the bid, with any necessary adjustments being made to the evaluation results, including the rank of the bid vis-à-vis other bids.

If no substitute is proposed the Contracting Authority will set aside the bid and give it no further consideration.

- (d) If a Bidder has proposed any individual who is not an employee of the Bidder, by submitting a bid, the Bidder certifies that it has the permission from that individual to propose his/her services in relation to the Work to be performed and to submit his/her résumé to Canada. The Bidder must, upon request from the Contracting Authority, provide a written confirmation, signed by the individual, of the permission given to the Bidder and of his/her availability. Failure to comply with the request may result in the bid being declared non-responsive.

5.1.3 Education and Experience

The Bidder certifies that all the information provided in the résumés and supporting material submitted with its bid, particularly the information pertaining to education, achievements, experience and work history, has been verified by the Bidder to be true and accurate. Furthermore, the Bidder warrants that every individual proposed by the Bidder for the requirement is capable of performing the Work described in the resulting contract.

5.1.4 Software Publisher Certification and Software Publisher Authorization

- (a) If the Bidder is the Software Publisher for any of the proprietary software component(s) it bids, Canada requires that the Bidder confirm in writing that it is the Software Publisher. Bidders are requested to use the Software Publisher Certification Form included with the bid solicitation. Although all the contents of the Software Publisher Certification Form are required, using the form itself to provide this information is not mandatory. For bidders who use an alternate form, it is in Canada's sole discretion to determine whether all the required information has been provided.
- (b) Any Bidder that is not the Software Publisher of all the proprietary software products or components proposed as part of its bid is required to submit proof of the Software Publisher's authorization, which must be signed by the Software Publisher (not the Bidder). No Contract will be awarded to a Bidder who is not the Software Publisher of all of the proprietary software it proposes to supply to Canada, unless proof of this authorization has been provided to Canada. If the proprietary software proposed by the Bidder originates with multiple Software Publishers, authorization is required from each Software Publisher. Bidders are requested to use the Software Publisher Authorization Form included with the bid solicitation. Although all the contents of the Software Publisher Authorization Form are required, using the form itself to provide this information is not mandatory. For Bidders/Software Publishers who use an alternate form, it is in Canada's sole discretion to determine whether all the required information has been provided.



- (c) In this bid solicitation, “Software Publisher” means the owner of the copyright in any software included in the bid, who has the right to license (and authorize others to license/sub-license) its software products.

5.1.5 Bidder Certifies that All Software is “Off-the-Shelf”

Any software bid to meet this requirement must be “off-the-shelf” (unless otherwise stated in this bid solicitation), meaning that each item of software is commercially available and requires no further research or development and is part of an existing product line with a field-proven operational history (that is, it has not simply been tested in a laboratory or experimental environment). If any of the software bid is a fully compatible extension of a field-proven product line, it must have been publicly announced on or before the bid closing date. By submitting a bid, the Bidder is certifying that all the software bid is off-the-shelf.

PART 6 – SECURITY AND OTHER REQUIREMENTS

6.1 Security Requirements

- (a) At the date of bid closing, the following conditions must be met:
- (i) the Bidder must hold a valid organization security clearance as indicated in Part 7 - Resulting Contract Clauses;
 - (ii) the Bidder's proposed individuals requiring access to classified or protected information, assets or sensitive work site(s) must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses;
 - (iii) the Bidder must provide the name of all individuals who will require access to classified or protected information, assets or sensitive work sites;
- (b) For additional information on security requirements, Bidders should refer to the [Industrial Security Program \(ISP\)](http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html) of Public Works and Government Services Canada (<http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html>) website.



PART 7 - RESULTING CONTRACT CLAUSES

The following clauses apply to and form part of any contract resulting from the bid solicitation.

7.1 Requirement

- (a) _____ (the Contractor) agrees to supply to the Client the goods and services described in the Contract, including the Statement of Work, in accordance with and at the prices set out in the Contract. This includes:
- (i) providing professional services, as requested by Canada;
 - (ii) granting the license to use the Licensed Software described in the Contract;
 - (iii) providing the Software Documentation; [*note: there is not a separate line item in the Basis of Payment provision for the Software Documentation - the price is included in the line item for Licensed Software; if you want to pay a separate price for the Software Documentation, be sure to add a separate paragraph in the Basis of Payment*]
 - (iv) providing maintenance and support services for the Licensed Software during the Software Support Period; and
 - (v) providing training, as and when requested by Canada.
- (b) **Client:** Under the Contract, the "Client" is Department of Finance.
- (c) **Reorganization of Client:** The Contractor's obligation to perform the Work will not be affected by (and no additional fees will be payable as a result of) the renaming, reorganization, reconfiguration, or restructuring of any Client. The reorganization, reconfiguration and restructuring of the Client includes the privatization of the Client, its merger with another entity, or its dissolution, where that dissolution is followed by the creation of another entity or entities with mandates similar to the original Client. In connection with any form of reorganization, Canada may designate another department or government body as the Contracting Authority or Technical Authority, as required to reflect the new roles and responsibilities associated with the reorganization.
- (d) **Defined Terms:** Words and expressions defined in the General Conditions or Supplemental General Conditions and used in the Contract have the meanings given to them in the General Conditions or Supplemental General Conditions.
- (i) any reference to a "**deliverable**" or "**deliverables**" includes the license to use the Licensed Software (the Licensed Software itself is not a deliverable, because the Licensed Software is only being licensed under the Contract, not sold or transferred).
- (e) **Location of Services:** Services must be delivered as requested to the locations specified in the Contract, which delivery locations must exclude any area subject to one of the Comprehensive Land Claim Agreements (CLCAs).

7.2 Minimum Work Guarantee

- (a) In this clause, "**Minimum Contract Value**" means 5% of the amount identified as the Total Estimated Cost on page 1 of the Contract when it is first awarded.
- (b) The Contractor must perform the Work described in the Contract as and when requested by Canada during the Contract Period. Canada's obligation under the Contract is to request Work in the amount of the Minimum Contract Value or, at Canada's option, to pay the Contractor at the end of the Contract in accordance with paragraph (c). In consideration of this obligation, the



Contractor agrees to stand in readiness throughout the Contract Period to perform the Work described in the Contract.

- (c) If Canada does not request work in the amount of the Minimum Contract Value during the Contract Period, Canada must pay the Contractor the difference between the Minimum Contract Value and the cost of the Work performed.
- (d) Canada will have no obligation to the Contractor under this clause if Canada terminates the Contract in whole or in part for default.

7.3 Standard Clauses and Conditions

All clauses and conditions identified in the Contract by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (<http://sacc.pwgsc.gc.ca/sacc/index-e.jsp>) issued by Public Works and Government Services Canada.

(a) **General Conditions:**

2035 (2016-04-04), General Conditions - Higher Complexity - Services, apply to and form part of the Contract.

(b) **Supplemental General Conditions :**

The following Supplemental General Conditions:

- (i) 4002 (2010-08-16), Supplemental General Conditions - Software Development or Modification Services;
- (ii) 4003 (2010-08-16) Supplemental General Conditions - Licensed Software
- (iii) 4004 (2013-04-25), Supplemental General Conditions - Maintenance and Support Services for Licensed Software;
- (iv) 4006 (2010-08-16), Supplemental General Conditions - Contractor to Own Intellectual Property Rights in Foreground Information;

7.4 Security Requirement

The Security Requirement Check List (SRCL and related clausings), as set out under Annex "C" applies.

Common PS SRCL #19 Summary:

- Access to PROTECTED and CLASSIFIED information and/or assets (Block 6a);
- Type of Information: CANADA (Block 7a);
- No release restrictions (Block 7b);
- Level of information – PROTECTED A, B, C, CONFIDENTIAL and SECRET (Block 7c);
- Personnel Security level – RELIABILITY STATUS, CONFIDENTIAL and SECRET (Block 10a);

Common PS SRCL #19 Security Clauses:

SECURITY REQUIREMENT FOR CANADIAN SUPPLIER: PWGSC FILE COMMON-PS-SRCL#19

1. The Contractor/Offeror must, at all times during the performance of the Contract/Standing Offer/Supply Arrangement, hold a valid Facility Security Clearance at the level of SECRET, issued by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services Canada (PWGSC).
2. The Contractor/Offeror personnel requiring access to PROTECTED/CLASSIFIED information, assets or sensitive work site(s) must EACH hold a valid personnel security screening at the level of **SECRET** as required, granted or approved by CISD/PWGSC.



3. The Contractor/Offeror MUST NOT remove any PROTECTED/CLASSIFIED information from the identified work site(s), and the Contractor/Offeror must ensure that its personnel are made aware of and comply with this restriction.
4. Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of CISD/PWGSC.
5. The Contractor/Offeror must comply with the provisions of the:
 - a. Security Requirements Check List and security guide (if applicable), attached at Annex _____;
 - b. *Industrial Security Manual* (Latest Edition).

7.5 Contract Period

- (a) **Contract Period:** The “**Contract Period**” is the entire period of time during which the Contractor is obliged to perform the Work, which includes:
- (i) The “**Initial Contract Period**”, which begins on the date the Contract is awarded and ends March 31, 2018.

7.6 Authorities

Administrative Authority:

- a) **The Administrative Authority for the Contract is:**

Name: Michelle Allen
 Telephone: 613-369-3460
 Address: 90 Elgin Street, Ottawa, ON K1A 0G5
 Email: michelle.allen@canada.ca

- b) **Contracting Authority (To be provided at Contract Award)**

The Contracting Authority for the Contract is:

Name: _____
 Title: _____
 Organization: _____
 Address: _____
 Telephone: _____
 Facsimile: _____
 E-mail address: _____

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

- c) **Technical Authority (To be provided at time of Contract award)**

The Technical Authority for the Contract is:

Name: _____
 Title: _____
 Organization: _____
 Address: _____
 Telephone: _____



Facsimile: _____
E-mail address: _____

The Technical Authority is the representative of the department or agency for whom the Work is being carried out under the Contract and is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Technical Authority; however, the Technical Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a contract amendment issued by the Contracting Authority.

d) **Contractor's Representative**

Name: _____
Title: _____
Organization: _____
Address: _____
Telephone: _____
Facsimile: _____
E-mail address: _____

7.7 Proactive Disclosure of Contracts with Former Public Servants

By providing information on its status, with respect to being a former public servant in receipt of a [Public Service Superannuation Act](#) (PSSA) pension, the Contractor has agreed that this information will be reported on departmental web sites as part of the published proactive disclosure reports, in accordance with [Contracting Policy Notice: 2012-2](#) of the Treasury Board Secretariat of Canada.

7.8 Payment

(a) **Basis of Payment**

Please see Annex B for detailed payment information.

- (i) **Licensed Software, Maintenance and Support:** For the license(s) to use the Licensed Software (including delivery, installation, integration and configuration of the Licensed Software and the Software Documentation in accordance with the Contract, Canada will pay the Contractor the firm price(s) set out in Annex B of this contract, FOB destination, including all customs duties, GST/HST extra. The firm prices include the warranty during the Software Warranty Period and maintenance and support during the Software Support Period (including for any additional licenses purchased during the Contract Period).
- (ii) **Optional Additional Software Licenses:** For additional licenses for additional Client Users to use the Licensed Software, if Canada exercises its option, Canada will pay the Contractor the firm price set out in Annex B of this contract FOB destination, including all customs duties, GST/HST extra.
- (iii) **Optional Software Support: If Canada exercises its** option to extend the Software Support Period, Canada will pay the Contractor the firm annual/monthly price set out in Annex ____ of this contract, FOB destination, including all customs duties, GST/HST extra.



- (iv) **Competitive Award:** The Contractor acknowledges that the Contract has been awarded as a result of a competitive process. No additional charges will be allowed to compensate for errors, oversights, misconceptions or underestimates made by the Contractor when bidding for the Contract.
- (v) **Professional Services Rates:** In Canada's experience, bidders from time to time propose rates at the time of bidding for one or more categories of resources that they later refuse to honour, on the basis that these rates do not allow them to recover their own costs and/or make a profit. This denies Canada of the benefit of the awarded contract. If the Contractor refuses, or is unable, to provide an individual with the qualifications described in the Contract within the time described in the Contract (or proposes instead to provide someone from an alternate category at a different rate), whether or not Canada terminates the Contract as a whole, Canada may impose sanctions or take other measures in accordance with the PWGSC Vendor Performance Policy (or equivalent) then in effect, which may include prohibiting the Contractor from bidding on future requirements that include any professional services, or rejecting the Contractor's other bids for professional services requirements on the basis that the Contractor's performance on this or other contracts is sufficiently poor to jeopardize the successful completion of other requirements.
- (vi) **Purpose of Estimates:** All estimated costs contained in the Contract are included solely for the administrative purposes of Canada and do not represent a commitment on the part of Canada to purchase services in these amounts. Any commitment to purchase specific amounts or values of services are described elsewhere in the Contract.

(b) **Limitation of Expenditure**

Canada will not pay the Contractor for any design changes, modifications or interpretations of the Work unless they have been approved, in writing, by the Contracting Authority before their incorporation into the Work.

(c) **Method of Payment**

(i) **Milestone Payments**

Canada will make milestone payments in accordance with the Schedule of Milestones detailed in the Contract and the payment provisions in Annex B.

- (A) all work associated with the milestone and as applicable any deliverable required has been completed and accepted by Canada.

(ii) **No Responsibility to Pay for Work not performed due to Closure of Government Offices**

Where the Contractor, its employees, subcontractors, or agents are providing services on government premises under the Contract and those premises are inaccessible because of the evacuation or closure of government offices, and as a result no work is performed, Canada is not responsible for paying the Contractor for work that otherwise would have been performed if there had been no evacuation or closure.

If, as a result of any strike or lock-out, the Contractor or its employees, subcontractors or agents cannot obtain access to government premises and, as a result, no work is performed, Canada is not responsible for paying the Contractor for work that otherwise would have been performed if the Contractor had been able to gain access to the premises.

7.9 Invoicing Instructions

- (a) The Contractor must submit invoices in accordance with the information required in the General Conditions.



- (b) The Contractor's invoice must include a separate line item for each subparagraph in the Basis of Payment provision.
- (c) By submitting invoices (other than for any items subject to an advance payment), the Contractor is certifying that the goods and services have been delivered and that all charges are in accordance with the Basis of Payment provision of the Contract, including any charges for work performed by subcontractors.
 - (i) The Contractor must provide the original of each invoice to the Technical Authority. On request, the Contractor must provide a copy of any invoices requested by the Contracting Authority.

7.10 Certifications

The continuous compliance with the certifications provided by the Contractor in its bid and the ongoing cooperation in providing additional information are conditions of the Contract. Certifications are subject to verification by Canada during the entire period of the Contract. If the Contractor does not comply with any certification, or fails to provide the additional information, or if it is determined that any certification made by the Contractor in its bid is untrue, whether made knowingly or unknowingly, Canada has the right, pursuant to the default provision of the Contract, to terminate the Contract for default.

7.11 Applicable Laws

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in the province of Ontario or as indicated in the Bidder's Supply Arrangement.

7.12 Priority of Documents

If there is a discrepancy between the wording of any documents that appear on the following list, the wording of the document that first appears on the list has priority over the wording of any document that appears later on the list:

- (a) these Articles of Agreement, including any individual SACC clauses incorporated by reference in these Articles of Agreement;
- (b) Supplemental general conditions, in the following order:

The following Supplemental General Conditions:

 - (i) [4002 \(2010-08-16\)](#), Supplemental General Conditions - Software Development or Modification Services;
 - (ii) [4003 \(2010-08-16\)](#), Supplemental General Conditions - Licensed Software
 - (iii) [4004 \(2013-04-25\)](#), Supplemental General Conditions - Maintenance and Support Services for Licensed Software;
 - (iv) [4006 \(2010-08-16\)](#), Supplemental General Conditions - Contractor to Own Intellectual Property Rights in Foreground Information;
- (c) General Conditions [2035 \(2016-04-04\)](#);
- (d) Annex A, Statement of Work;
- (e) Annex B, Basis of Payment;
- (f) Annex C, Security Requirements Check List;
- (g) Annex __, Additional Software Use Terms Approved by Canada (if any), which are only binding on Canada if they have been initialed by both parties in the signed copy of the Contract (*if required by the RFP*);
- (h) the Contractor's bid dated _____ (insert date of bid), as amended _____ (insert date(s) of amendment(s) if applicable), not including any software publisher license terms and conditions



that may be included in the bid, not including any provisions in the bid with respect to limitations on liability, and not including any terms and conditions incorporated by reference (including by way of a web link) in the bid.

7.13 Limitation of Liability - Information Management/Information Technology

- (a) This section applies despite any other provision of the Contract and replaces the section of the general conditions entitled "Liability". Any reference in this section to damages caused by the Contractor also includes damages caused by its employees, as well as its subcontractors, agents, and representatives, and any of their employees. This section applies regardless of whether the claim is based in contract, tort, or another cause of action. The Contractor is not liable to Canada with respect to the performance of or failure to perform the Contract, except as described in this section and in any section of the Contract pre-establishing any liquidated damages. The Contractor is only liable for indirect, special or consequential damages to the extent described in this Article, even if it has been made aware of the potential for those damages.
- (b) **First Party Liability:**
- (i) The Contractor is fully liable for all damages to Canada, including indirect, special or consequential damages, caused by the Contractor's performance or failure to perform the Contract that relate to:
 - (A) any infringement of intellectual property rights to the extent the Contractor breaches the section of the General Conditions entitled "Intellectual Property Infringement and Royalties";
 - (B) physical injury, including death.
 - (ii) The Contractor is liable for all direct damages caused by the Contractor's performance or failure to perform the Contract affecting real or tangible personal property owned, possessed, or occupied by Canada.
 - (iii) Each of the Parties is liable for all direct damages resulting from its breach of confidentiality under the Contract. Each of the Parties is also liable for all indirect, special or consequential damages in respect of its unauthorized disclosure of the other Party's trade secrets (or trade secrets of a third party provided by one Party to another under the Contract) relating to information technology.
 - (iv) The Contractor is liable for all direct damages relating to any encumbrance or claim relating to any portion of the Work for which Canada has made any payment. This does not apply to encumbrances or claims relating to intellectual property rights, which are addressed under (i)(A) above.
 - (v) The Contractor is also liable for any other direct damages to Canada caused by the Contractor's performance or failure to perform the Contract that relate to:
 - (A) any breach of the warranty obligations under the Contract, up to the total amount paid by Canada (including any applicable taxes) for the goods and services affected by the breach of warranty; and
 - (B) any other direct damages, including all identifiable direct costs to Canada associated with re-procuring the Work from another party if the Contract is terminated by Canada either in whole or in part for default, up to an aggregate maximum for this subparagraph (B) of the greater of 0.75 times the total estimated cost (meaning the dollar amount shown on the first page of the Contract in the cell titled "Total Estimated Cost" or shown on each call-up, purchase order or other document used to order goods or services under this instrument), or \$1,000,000.00.



In any case, the total liability of the Contractor under subparagraph (v) will not exceed the total estimated cost (as defined above) for the Contract or \$1,000,000.00, whichever is more.

- (vi) If Canada's records or data are harmed as a result of the Contractor's negligence or willful act, the Contractor's only liability is, at the Contractor's own expense, to restore Canada's records and data using the most recent back-up kept by Canada. Canada is responsible for maintaining an adequate back-up of its records and data.

(c) **Third Party Claims:**

- (i) Regardless of whether a third party makes its claim against Canada or the Contractor, each Party agrees that it is liable for any damages that it causes to any third party in connection with the Contract as set out in a settlement agreement or as finally determined by a court of competent jurisdiction, where the court determines that the Parties are jointly and severally liable or that one Party is solely and directly liable to the third party. The amount of the liability will be the amount set out in the settlement agreement or determined by the court to have been the Party's portion of the damages to the third party. No settlement agreement is binding on a Party unless its authorized representative has approved the agreement in writing.
- (ii) If Canada is required, as a result of joint and several liability or joint and solidarily liable, to pay a third party in respect of damages caused by the Contractor, the Contractor must reimburse Canada by the amount finally determined by a court of competent jurisdiction to be the Contractor's portion of the damages to the third party. However, despite Sub-article (i), with respect to special, indirect, and consequential damages of third parties covered by this Section, the Contractor is only liable for reimbursing Canada for the Contractor's portion of those damages that Canada is required by a court to pay to a third party as a result of joint and several liability that relate to the infringement of a third party's intellectual property rights; physical injury of a third party, including death; damages affecting a third party's real or tangible personal property; liens or encumbrances on any portion of the Work; or breach of confidentiality.
- (iii) The Parties are only liable to one another for damages to third parties to the extent described in this Sub-article (c).

7.14 Joint Venture Contractor

- (a) The Contractor confirms that the name of the joint venture is _____ and that it is comprised of the following members: ***[list all the joint venture members named in the Contractor's original bid]***
- (b) With respect to the relationship among the members of the joint venture Contractor, each member agrees, represents and warrants (as applicable) that:
 - (i) _____ has been appointed as the "representative member" of the joint venture Contractor and has fully authority to act as agent for each member regarding all matters relating to the Contract;
 - (ii) by giving notice to the representative member, Canada will be considered to have given notice to all the members of the joint venture Contractor; and
 - (iii) all payments made by Canada to the representative member will act as a release by all the members.
- (c) All the members agree that Canada may terminate the Contract in its discretion if there is a dispute among the members that, in Canada's opinion, affects the performance of the Work in any way.



- (d) All the members are jointly and severally or solidarily liable for the performance of the entire Contract.
- (e) The Contractor acknowledges that any change in the membership of the joint venture (i.e., a change in the number of members or the substitution of another legal entity for an existing member) constitutes an assignment and is subject to the assignment provisions of the General Conditions.
- (f) The Contractor acknowledges that all security and controlled goods requirements in the Contract, if any, apply to each member of the joint venture Contractor.

Note to Bidders: *This Article will be deleted if the bidder awarded the contract is not a joint venture. If the contractor is a joint venture, this clause will be completed with information provided in its bid.*

7.15 Licensed Software

- (a) With respect to the provisions of Supplemental General Conditions 4003 (2010-08-16):

Licensed Software	The Licensed Software, which is defined in 4003, includes all the products offered by the Contractor in its bid, and any other software code required for those products to function in accordance with the Software Documentation and the Specifications, including without limitation all of the following products: _____ [this information will be completed at contract award using information in the Contractor's bid]
Type of License being Granted	Device license
Number of Devices Licensed	35
Option to Purchase Licenses for Additional Devices	The Contractor grants to Canada the irrevocable option to purchase licenses for additional Devices at the price set out in Annex B on the same terms and conditions as the initial Device licenses granted under the Contract. This option may be exercised at any time during the Contract Period, as many times as Canada chooses. This option may only be exercised by the Contracting Authority by notice in writing and will be evidenced, for administrative purposes only, by a contract amendment.
Language of Licensed Software	The Licensed Software must be delivered in both French and English.
Delivery Location	90 Elgin, Ottawa, ON K1A 0G5
Installation Site	90 Elgin, Ottawa, ON K1A 0G5
Media on which Licensed Software must be Delivered	CD-ROM or Internet Download.
Term of License	Term of license 1 year

7.16 Licensed Software Maintenance and Support

- (a) With respect to the provisions of Supplemental General Conditions 4004 (2013-04-25):



Software Support Period	1 year from date where software is fully operational and functional.
Software Support Period when Additional Licenses added during Contract Period	For any additional licenses purchased in accordance with the Contract, the Software Support Period currently underway will apply to the additional licenses purchased, so that the Software Support Period ends on the same date for all licences supported under the Contract.
Hours for Providing Support Services	The Contractor's personnel must be available from 7:30 a.m. until 5 p.m., local time, at the site where the Licensed Programs are installed, via telephone access, Monday through Friday, exclusive of statutory holidays observed by Canada at the site where the service is required.
Contractor must provide On-site Support Services	No
Contact Information for Accessing the Contractor's Support Services	In accordance with Section 5 of 4004, the Contractor will make its Support Services available through the following: Toll-free Telephone Access: _____ On-line Portal: _____ Toll-free Fax Access: not required Email Access: not required The Contractor must respond to all telephone communications (with a live service agent) within 60 minutes of the initial time of the Client or User's initial communication. <i>[Note to Bidders: This information will be completed at the time of contract award with information supplied by the Contractor. Bidders are requested to provide this information in their bids.]</i>
Language of Support Services	The Support Services must be provided in both French and English, based on the choice of the User requesting support.

7.17 Training

(a) Providing Software Training

- (i) The Contractor must provide on-site training on the software products that form part of the Software Solution on an "as-and-when-requested" basis during the Contract Period. The Contractor must provide training as required.

7.18 Professional Services - General

- (a) The Contractor must provide professional services on request as specified in this contract.

All resources provided by the Contractor must meet the qualifications described in the Contract (including those relating to previous experience, professional designation, education, language proficiency and security clearance) and must be competent to provide the required services by any delivery dates described in the Contract.

- (b) If the Contractor fails to deliver any deliverable (excluding delivery of an individual) or complete any task described in the Contract on time, in addition to any other rights or remedies available to Canada under the Contract or the law, Canada may notify the Contractor of the deficiency, in which case the Contractor must submit a written plan to the Technical Authority within ten working



days detailing the actions that the Contractor will undertake to remedy the deficiency. The Contractor must prepare and implement the plan at its own expense.

- (c) In General Conditions 2035 (2016-04-04), Section 08 titled "Replacement of Specific Individuals" is deleted and the following applies instead:

Replacement of Specific Individuals

- (i) If the Contractor is unable to provide the services of any specific individual identified in the Contract to perform the services, the Contractor must within five working days of the individual's departure or failure to commence Work (or, if Canada has requested the replacement, within ten working days of Canada's notice of the requirement for a replacement) provide to the Contracting Authority:
- (A) the name, qualifications and experience of a proposed replacement immediately available for Work; and
 - (B) security information on the proposed replacement as specified by Canada, if applicable.

The replacement must have qualifications and experience that meet or exceed the score obtained for the original resource.

- (ii) Subject to an Excusable Delay, where Canada becomes aware that a specific individual identified under the Contract to provide the services has not been provided or is not performing, the Contracting Authority may elect to:
- (A) exercise Canada's rights or remedies under the Contract or at law, including terminating the Contract in whole or in part for default under the Section titled "Default of the Contractor", or
 - (B) assess the information provided under (c) (i) above or, if it has not yet been provided, require the Contractor propose a replacement to be rated by the Technical Authority. The replacement must have qualifications and experience that meet or exceed those obtained for the original resource and be acceptable to Canada. Upon assessment of the replacement, Canada may accept the replacement, exercise the rights in (ii) (A) above, or require another replacement in accordance with this subarticle (c).

Where an Excusable Delay applies, Canada may require (c) (ii) (B) above instead of terminating under the Excusable Delay Section. An Excusable Delay does not include resource unavailability due to allocation of the resource to another Contract or project (including those for the Crown) being performed by the Contractor or any of its affiliates.

- (iii) The Contractor must not, in any event, allow performance of the Work by unauthorized replacement persons. The Contracting Authority may order that an original or replacement resource stop performing the Work. In such a case, the Contractor must immediately comply with the order. The fact that the Contracting Authority does not order that a resource stop performing the Work does not relieve the Contractor from its responsibility to meet the requirements of the Contract.
- (iv) The obligations in this article apply despite any changes that Canada may have made to the Client's operating environment.

7.19 Safeguarding Electronic Media

- (a) Before using them on Canada's equipment or sending them to Canada, the Contractor must use a regularly updated product to scan electronically all electronic media used to perform the Work for computer viruses and other coding intended to cause malfunctions. The Contractor must notify



Canada if any electronic media used for the Work are found to contain computer viruses or other coding intended to cause malfunctions.

- (b) If magnetically recorded information or documentation is damaged or lost while in the Contractor's care or at any time before it is delivered to Canada in accordance with the Contract, including accidental erasure, the Contractor must immediately replace it at its own expense.

7.20 Representations and Warranties

The Contractor made statements regarding its and its proposed resources experience and expertise in its bid that resulted in the award of the Contract. The Contractor represents and warrants that all those statements are true and acknowledges that Canada relied on those statements in awarding the Contract. The Contractor also represents and warrants that it has, and all its resources and subcontractors that perform the Work have, and at all times during the Contract Period they will have, the skills, qualifications, expertise and experience necessary to perform and manage the Work in accordance with the Contract, and that the Contractor (and any resources or subcontractors it uses) has previously performed similar services for other customers.

7.21 Access to Canada's Property and Facilities

Canada's property, facilities, equipment, documentation, and personnel are not automatically available to the Contractor. If the Contractor would like access to any of these, it is responsible for making a request to the Technical Authority. Unless expressly stated in the Contract, Canada has no obligation to provide any of these to the Contractor. If Canada chooses, in its discretion, to make its property, facilities, equipment, documentation or personnel available to the Contractor to perform the Work, Canada may require an adjustment to the Basis of Payment and additional security requirements may apply.

7.22 Government Property

Canada agrees to supply the Contractor with the items listed below (the "**Government Property**"). The section of the General Conditions entitled "Government Property" also applies to the use of the Government Property by the Contractor.

7.23 Implementation

- (a) **Finalization of Draft Implementation Plan:** Within *10 working days* of the Contract being awarded, Canada will provide any comments it has regarding the draft implementation plan submitted by the Contractor as part of its bid. The Contractor must update the implementation plan to reflect Canada's comments within *5 working days* and resubmit it to Canada for approval.



ANNEX "A" - STATEMENT OF WORK

IT SERVICE MANAGEMENT SOFTWARE TOOL AND PROFESSIONAL SERVICES

1.0 OBJECTIVE

The Department of Finance (FIN) requires an Information Management (IT) Service Management software and the services of a Contractor to install and configure the software. This software will be used by FIN IT Client Service Unit to administer daily client IT requests. The Contractor must provide training, integration and customization services associated with the proposed IT Service Management software.

2.0 BACKGROUND

The Department of Finance's current IT Service Management software solution will be decommissioned on December 31, 2017. A new IT Service Management software solution is required prior to this date.

3.0 CONTRACT PERIOD

The initial contract period will be from date of contract award to March 31, 2018.

Software: Licensing will be either on a yearly basis or a one-time charge, which includes technical support and on-going maintenance. 35 licenses are required.

4.0 SOFTWARE REQUIREMENTS

The Contractors proposed IT Software solution must contain the following modules:

1. Incident and problem management

Software must initiate, route, track, and manage incidents, create and link different ticket types as well as has the ability to report on key performance indicators.

2. Request management

Software must log, track and report on users' requests, create and assign tasks and subtasks, manage users and contact information as well as has the ability to report on key indicators.

3. Asset management

Software must manage and track all configuration items and assets of an organization. Has the ability to report on key performance indicators.

4. Service Catalogue

Software must manage and report on IT services delivered to client organizations.

5. Self-Service

Software must allow users to automatically open a ticket against given categories.

6. Reports and Dashboards

Software must provide summary of incidents, problems and assets and have a database and reporting structure that is cross-functional across all modules with predefined key performance indicators based on ITILv3 best practices.



7. Workflow

Software must automate pre-defined tasks, route tickets and manage approvals. Has the ability to modify current services and supporting workflows without the need for specialized programming.

5.0 DELIVERABLES & TASKS

Deliverables	Task	Deadline
Software Installation	Install Software, Assist with Active Directory, SMTP email, integration,	November 30, 2016
Configuration of software modules	Configure the following modules; Incident Management and Problem Management; Self-Serve; Asset Management; Customizable reports and Dashboards; Service Catalogue; Workflows and Approvals; provide FIN IT employees with training and training material.	December 31, 2016
Upload current information into new tool.	Assets, employee first/last name, office number, branch and division, phone number, username, title, etc.	December 31, 2016
Information Flow Enforcement	The software enforces approved authorizations for controlling the flow of information within the system and between interconnected systems. The vendor is required to work closely with FIN and SSC IT groups to define specific architectural solutions in support of this requirement.	March 31, 2017
Developing CONOPS and remediating vulnerabilities (if any)found in the Vulnerability Assessment	Develop CONOPS document for IT Security review and assessment at the end of the design phase	March 31, 2017
Vulnerability Scanning	FIN IT Security will scan for application level vulnerabilities in all the software and infrastructure components at the end of the development / integration phase. The vendor is required to analyze the vulnerability scan reports and remediate all legitimate vulnerabilities.	March 31, 2017
Assist with testing and correction of any errors	The vendor will be on-site assisting with correcting vulnerabilities and/or errors found during Vulnerability/UAT testing and provide guidance.	March 31, 2017
Assist and provide full training to FIN-IT employees on the	Full training manual to be provided by supplier.	March 31, 2017



administration of the tool across all modules		
--	--	--

6.0 TECHNICAL ENVIRONMENT

The general business network is a Microsoft based network using Microsoft Hyper-V virtualization technology hosting client laptop computer devices. It provides departmental web site hosting; internet browsing, e-mail, Blackberry, remote access and file and print services. The network operates at Protected B level.

This network is built on Microsoft's integrated software technology which includes but is not limited to:

- **Windows 7 desktops**
- **MS Office 2010**
- **Remote Access, such as G-On keys or Entrust PKI**
- **Adobe Reader XI**
- **Entrust 9.3**
- **MS SCCM**
- **MS Active Directory**
- **Windows File / Print Server**
- **Microsoft SQL Server 2008/2012**
- **IIS version 7 and version 8**

Computer equipment and access to the networks will be provided as required. Non FIN equipment is not to be connected to the FIN network.

Any software not already available on the networks must be approved by the Department of Finance and Shared Services Canada prior to installation.

Email integration will consist in identifying an SMTP gateway in collaboration with Shared Service Canada and the configuration of email services within the software.

Active Directory integration will consist in providing system single sign-on capability and populating employee information to be available in the ITSM tool, such as:

- First name, last name
- Branch and division
- Phone Number
- Office Location
- Title

7.0 PROJECT AUTHORITY

The name and contact information of the Department of Finance Project Authority will be released at the time of contract award.

8.0 RESPONSIBILITIES

All work will be carried out in close consultation with the Project Authority and / or their technical staff.

Department of Finance Responsibilities:

The Project Authority will:

- Inform the Contractor of any activity that may affect the project deliverables or deadlines.
- Provide access to Departmental networks.
- Provide regular feedback to Contractor on emerging issues or concerns.



Contractor Responsibilities:

The Contractor will:

- Communicate promptly with the Project Authority regarding any issue or obstacle beyond the Contractor's control that may hinder the Contractor or its resource's ability to complete the tasks and deliver the deliverables as outlined in this Statement of Work
- Assist the Project Authority and resources in resolving issues that may arise during the performance of the work

9.0 WORK LOCATION

All work will be carried out at the Department of Finance offices located at 90 Elgin Street, Ottawa ON K1A 0G5.

10.0 SECURITY REQUIREMENTS

The Contractor must hold a valid Government of Canada Supplier Security Clearance at the level of Secret throughout the duration of the contract.

The Contractor's resources must hold a valid Government of Canada personnel security clearance at the level of Secret throughout the duration of the contract.

The Contractor's proposed IT Solutions Software must meet the IT Security requirements identified in 7.4 (attached).

11.0 TRAVEL

All the work associated with this SOW is to be carried out in the National Capital Region (NCR). The Department of Finance will not reimburse any travel costs within or outside the NCR, including those incurred by the resource.



ANNEX “B” - BASIS OF PAYMENT

The Contractor will be paid in accordance with the following Basis of Payment for work performed under the Contract.

The Contractor will be paid the following firm all-inclusive prices for work performed under this Contract, in accordance with Annex “A” – Statement of Work, during the Contract period, Harmonized Sales Tax (HST) extra.

Payment will be made upon completion and acceptance of each Milestone as indicated below.

Milestones	Deliverables	Description	Deadline	Fixed Price Cost
1	Software (license)	Provide 35 device licenses with one year maintenance and support.	November 30, 2016	
2	Software Installation	Install Software, Assist with Active Directory, SMTP email, integration	November 30, 2016	
3	Configuration of software modules	Configure the following modules; Incident Management and Problem Management; Self-Serve; Asset Management; Customizable reports and Dashboards; Service Catalogue; Workflows and Approvals; provide FIN IT employees with training and training material.	December 31, 2016	
4	Upload current information into new tool.	Assets, employee first/last name, office number, branch and division, phone number, username, title, etc.	December 31, 2016	
5	Information Flow Enforcement	The software enforces approved authorizations for controlling the flow of information within the system and between interconnected systems. The vendor is required to work closely with FIN and SSC IT groups to define specific architectural solutions in support of this requirement.	March 31, 2017	
6	Developing CONOPS and remediating vulnerabilities (if any)found in the Vulnerability Assessment	Develop CONOPS document for IT Security review and assessment at the end of the design phase	March 31, 2017	



7	Vulnerability Scanning	FIN IT Security will scan for application level vulnerabilities in all the software and infrastructure components at the end of the development / integration phase. The vendor is required to analyze the vulnerability scan reports and remediate all legitimate vulnerabilities.	March 31, 2017	
8	Assist with testing and correction of any errors	The vendor will be on-site assisting with correcting vulnerabilities and/or errors found during Vulnerability/UAT testing and provide guidance.	March 31, 2017	
9	Assist and provide full training to FIN-IT employees on the administration of the tool across all modules	Full training manual to be provided by supplier	March 31, 2017	

Optional Pricing for additional licenses:

Deliverables	Description	Fixed Price Cost Per License
Software (license)	Provide additional device licenses with pro-rated maintenance and support.	



ANNEX "C" - SECURITY REQUIREMENTS CHECK LIST

As per the attached SRCL



Contract Number / Numéro du contrat
Security Classification / Classification de sécurité

**SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)**

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine	2. Branch or Directorate / Direction générale ou Direction
3. a) Subcontract Number / Numéro du contrat de sous-traitance	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant

4. Brief Description of Work / Brève description du travail

5. a) Will the supplier require access to Controlled Goods?
Le fournisseur aura-t-il accès à des marchandises contrôlées? No / Non Yes / Oui

5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations?
Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques? No / Non Yes / Oui

6. Indicate the type of access required / Indiquer le type d'accès requis

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets?
Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS?
(Specify the level of access using the chart in Question 7. c)
(Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c) No / Non Yes / Oui

6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted.
Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé. No / Non Yes / Oui

6. c) Is this a commercial courier or delivery requirement with **no** overnight storage?
S'agit-il d'un contrat de messagerie ou de livraison commerciale **sans** entreposage de nuit? No / Non Yes / Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada <input type="checkbox"/>	NATO / OTAN <input type="checkbox"/>	Foreign / Étranger <input type="checkbox"/>
---------------------------------	--------------------------------------	---

7. b) Release restrictions / Restrictions relatives à la diffusion

No release restrictions Aucune restriction relative à la diffusion <input type="checkbox"/>	All NATO countries Tous les pays de l'OTAN <input type="checkbox"/>	No release restrictions Aucune restriction relative à la diffusion <input type="checkbox"/>
Not releasable À ne pas diffuser <input type="checkbox"/>		
Restricted to: / Limité à : <input type="checkbox"/> Specify country(ies): / Préciser le(s) pays :	Restricted to: / Limité à : <input type="checkbox"/> Specify country(ies): / Préciser le(s) pays :	Restricted to: / Limité à : <input type="checkbox"/> Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

PROTECTED A PROTÉGÉ A <input type="checkbox"/>	NATO UNCLASSIFIED NATO NON CLASSIFIÉ <input type="checkbox"/>	PROTECTED A PROTÉGÉ A <input type="checkbox"/>
PROTECTED B PROTÉGÉ B <input type="checkbox"/>	NATO RESTRICTED NATO DIFFUSION RESTREINTE <input type="checkbox"/>	PROTECTED B PROTÉGÉ B <input type="checkbox"/>
PROTECTED C PROTÉGÉ C <input type="checkbox"/>	NATO CONFIDENTIAL NATO CONFIDENTIEL <input type="checkbox"/>	PROTECTED C PROTÉGÉ C <input type="checkbox"/>
CONFIDENTIAL CONFIDENTIEL <input type="checkbox"/>	NATO SECRET NATO SECRET <input type="checkbox"/>	CONFIDENTIAL CONFIDENTIEL <input type="checkbox"/>
SECRET SECRET <input type="checkbox"/>	COSMIC TOP SECRET COSMIC TRÈS SECRET <input type="checkbox"/>	SECRET SECRET <input type="checkbox"/>
TOP SECRET TRÈS SECRET <input type="checkbox"/>		TOP SECRET TRÈS SECRET <input type="checkbox"/>
TOP SECRET (SIGINT) TRÈS SECRET (SIGINT) <input type="checkbox"/>		TOP SECRET (SIGINT) TRÈS SECRET (SIGINT) <input type="checkbox"/>

Security Classification / Classification de sécurité
--



Contract Number / Numéro du contrat
Security Classification / Classification de sécurité

PART A (continued) / PARTIE A (suite)

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets?
 Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS? No / Non Yes / Oui
 If Yes, indicate the level of sensitivity:
 Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets?
 Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate? No / Non Yes / Oui
 Short Title(s) of material / Titre(s) abrégé(s) du matériel :
 Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

<input type="checkbox"/> RELIABILITY STATUS COTE DE FIABILITÉ	<input type="checkbox"/> CONFIDENTIAL CONFIDENTIEL	<input type="checkbox"/> SECRET SECRET	<input type="checkbox"/> TOP SECRET TRÈS SECRET
<input type="checkbox"/> TOP SECRET-SIGINT TRÈS SECRET - SIGINT	<input type="checkbox"/> NATO CONFIDENTIAL NATO CONFIDENTIEL	<input type="checkbox"/> NATO SECRET NATO SECRET	<input type="checkbox"/> COSMIC TOP SECRET COSMIC TRÈS SECRET
<input type="checkbox"/> SITE ACCESS ACCÈS AUX EMBLEMES			

Special comments:
 Commentaires spéciaux : _____

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
 REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work?
 Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail? No / Non Yes / Oui
 If Yes, will unscreened personnel be escorted?
 Dans l'affirmative, le personnel en question sera-t-il escorté? No / Non Yes / Oui

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises?
 Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS? No / Non Yes / Oui

11. b) Will the supplier be required to safeguard COMSEC information or assets?
 Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC? No / Non Yes / Oui

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises?
 Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ? No / Non Yes / Oui

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data?
 Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS? No / Non Yes / Oui

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency?
 Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale? No / Non Yes / Oui



PART C - (continued) / PARTIE C - (suite)

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.

Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the Internet), the summary chart is automatically populated by your responses to previous questions.

Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ			CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET
											A	B	C			
Information / Assets / Renseignements / Biens / Production																
IT Media / Support TI																
IT Link / Lien électronique																

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED? No Yes
 La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE? Non Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifiez le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED? No Yes
 La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE? Non Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifiez le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquez qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).



Contract Number / Numéro du contrat
Security Classification / Classification de sécurité

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme			
Name (print) - Nom (en lettres moulées)		Title - Titre	Signature
Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
14. Organization Security Authority / Responsable de la sécurité de l'organisme			
Name (print) - Nom (en lettres moulées)		Title - Titre	Signature
Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached? Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?			<input type="checkbox"/> No / Non <input type="checkbox"/> Yes / Oui
16. Procurement Officer / Agent d'approvisionnement			
Name (print) - Nom (en lettres moulées) Michelle Allen		Title - Titre Contracting and Procurement Officer	Signature
Telephone No. - N° de téléphone 613-369-3460	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel Michelle.allen@canada.ca	Date
17. Contracting Security Authority / Autorité contractante en matière de sécurité			
Name (print) - Nom (en lettres moulées)		Title - Titre	Signature
Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date

Security Classification / Classification de sécurité
--

Instructions for completion of a Security Requirements Check List (SRCL)

The instruction sheet should remain attached until Block #17 has been completed.

GENERAL - PROCESSING THIS FORM

The project authority shall arrange to complete this form.

The organization security officer shall review and approve the security requirements identified in the form, in cooperation with the project authority.

The contracting security authority is the organization responsible for ensuring that the suppliers are compliant with the security requirements identified in the SRCL.

All requisitions and subsequent tender / contractual documents including subcontracts that contain PROTECTED and/or CLASSIFIED requirements must be accompanied by a completed SRCL.

It is important to identify the level of PROTECTED information or assets as Level "A," "B" or "C," when applicable; however, certain types of information may only be identified as "PROTECTED". No information pertaining to a PROTECTED and/or CLASSIFIED government contract may be released by suppliers, without prior written approval of the individual identified in Block 17 of this form.

The classification assigned to a particular stage in the contractual process does not mean that everything applicable to that stage is to be given the same classification. Every item shall be PROTECTED and/or CLASSIFIED according to its own content. If a supplier is in doubt as to the actual level to be assigned, they should consult with the individual identified in Block 17 of this form.

PART A - CONTRACT INFORMATION

Contract Number (top of the form)

This number must be the same as that found on the requisition and should be the one used when issuing an RFP or contract. This is a unique number (i.e. no two requirements will have the same number). A new SRCL must be used for each new requirement or requisition (e.g. new contract number, new SRCL, new signatures).

1. Originating Government Department or Organization

Enter the department or client organization name or the prime contractor name for which the work is being performed.

2. Directorate / Branch

This block is used to further identify the area within the department or organization for which the work will be conducted.

3. a) Subcontract Number

If applicable, this number corresponds to the number generated by the Prime Contractor to manage the work with its subcontractor.

b) Name and Address of Subcontractor

Indicate the full name and address of the Subcontractor if applicable.

4. Brief Description of Work

Provide a brief explanation of the nature of the requirement or work to be performed.

5. a) Will the supplier require access to Controlled Goods?

*The Defence Production Act (DPA) defines "Controlled Goods" as certain goods listed in the Export Control List, a regulation made pursuant to the *Export and Import Permits Act* (EIPA). Suppliers who examine, possess, or transfer Controlled Goods within Canada must register in the Controlled Goods Directorate or be exempt from registration. More information may be found at www.cgd.gc.ca.*

b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations?

The prime contractor and any subcontractors must be certified under the U.S./Canada Joint Certification Program if the work involves access to unclassified military data subject to the provisions of the Technical Data Control Regulations. More information may be found at www.dlis.dla.mil/jcp.

6. Indicate the type of access required

Identify the nature of the work to be performed for this requirement. The user is to select one of the following types:

a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets?

The supplier would select this option if they require access to PROTECTED and/or CLASSIFIED information or assets to perform the duties of the requirement.

b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted.

The supplier would select this option if they require regular access to government premises or a secure work site only. The supplier will not have access to PROTECTED and/or CLASSIFIED information or assets under this option.

c) Is this a commercial courier or delivery requirement with no overnight storage?

The supplier would select this option if there is a commercial courier or delivery requirement. The supplier will not be allowed to keep a package overnight. The package must be returned if it cannot be delivered.

7. Type of information / Release restrictions / Level of information

Identify the type(s) of information that the supplier may require access to, list any possible release restrictions, and if applicable, provide the level(s) of the information. The user can make multiple selections based on the nature of the work to be performed.

Departments must process SRCLs through PWGSC where:

- contracts that afford access to PROTECTED and/or CLASSIFIED foreign government information and assets;
- contracts that afford foreign contractors access to PROTECTED and/or CLASSIFIED Canadian government information and assets; or
- contracts that afford foreign or Canadian contractors access to PROTECTED and/or CLASSIFIED information and assets as defined in the documents entitled Identifying INFOSEC and INFOSEC Release.

a) Indicate the type of information that the supplier will be required to access

Canadian government information and/or assets

If Canadian information and/or assets are identified, the supplier will have access to PROTECTED and/or CLASSIFIED information and/or assets that are owned by the Canadian government.

NATO information and/or assets

If NATO information and/or assets are identified, this indicates that as part of this requirement, the supplier will have access to PROTECTED and/or CLASSIFIED information and/or assets that are owned by NATO governments. NATO information and/or assets are developed and/or owned by NATO countries and are not to be divulged to any country that is not a NATO member nation. Persons dealing with NATO information and/or assets must hold a NATO security clearance and have the required need-to-know.

Requirements involving CLASSIFIED NATO information must be awarded by PWGSC. PWGSC / CIISD is the Designated Security Authority for industrial security matters in Canada.

Foreign government information and/or assets

If foreign information and/or assets are identified, this requirement will allow access to information and/or assets owned by a country other than Canada.

b) Release restrictions

If **Not Releasable** is selected, this indicates that the information and/or assets are for **Canadian Eyes Only (CEO)**. Only Canadian suppliers based in Canada can bid on this type of requirement. NOTE: If Canadian information and/or assets coexists with CEO information and/or assets, the CEO information and/or assets must be stamped **Canadian Eyes Only (CEO)**.

If **No Release Restrictions** is selected, this indicates that access to the information and/or assets are not subject to any restrictions.

If **ALL NATO countries** is selected, bidders for this requirement must be from NATO member countries only.

NOTE: There may be multiple release restrictions associated with a requirement depending on the nature of the work to be performed. In these instances, a security guide should be added to the SRCL clarifying these restrictions. The security guide is normally generated by the organization's project authority and/or security authority.

c) Level of information

Using the following chart, indicate the appropriate level of access to information/assets the supplier must have to perform the duties of the requirement.

PROTECTED	CLASSIFIED	NATO
PROTECTED A	CONFIDENTIAL	NATO UNCLASSIFIED
PROTECTED B	SECRET	NATO RESTRICTED
PROTECTED C	TOP SECRET	NATO CONFIDENTIAL
	TOP SECRET (SIGINT)	NATO SECRET
		COSMIC TOP SECRET

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets?

If Yes, the supplier personnel requiring access to COMSEC information or assets must receive a COMSEC briefing. The briefing will be given to the "holder" of the COMSEC information or assets. In the case of a "personnel assigned" type of contract, the customer department will give the briefing. When the supplier is required to receive and store COMSEC information or assets on the supplier's premises, the supplier's COMSEC Custodian will give the COMSEC briefings to the employees requiring access to COMSEC information or assets. If Yes, the Level of sensitivity must be indicated.

9. Will the supplier require access to extremely sensitive INFOSEC information or assets?

If Yes, the supplier must provide the Short Title of the material and the Document Number. Access to extremely sensitive INFOSEC information or assets will require that the supplier undergo a Foreign Ownership Control or Influence (FOCI) evaluation by CIISD.

PART B - PERSONNEL (SUPPLIER)

10. a) Personnel security screening level required

Identify the screening level required for access to the information/assets or client facility. More than one level may be identified depending on the nature of the work. Please note that Site Access screenings are granted for access to specific sites under prior arrangement with the Treasury Board of Canada Secretariat. A Site Access screening only applies to individuals, and it is not linked to any other screening level that may be granted to individuals or organizations.

RELIABILITY STATUS	CONFIDENTIAL	SECRET
TOP SECRET	TOP SECRET (SIGINT)	NATO CONFIDENTIAL
NATO SECRET	COSMIC TOP SECRET	SITE ACCESS

If multiple levels of screening are identified, a Security Classification Guide must be provided.

b) May unscreened personnel be used for portions of the work?

Indicating Yes means that portions of the work are not PROTECTED and/or CLASSIFIED and may be performed outside a secure environment by unscreened personnel. The following question must be answered if unscreened personnel will be used:

Will unscreened personnel be escorted?

If No, unscreened personnel may not be allowed access to sensitive work sites and must not have access to PROTECTED and/or CLASSIFIED information and/or assets.

If Yes, unscreened personnel must be escorted by an individual who is cleared to the required level of security in order to ensure there will be no access to PROTECTED and/or CLASSIFIED information and/or assets at the work site.

PART C - SAFEGUARDS (SUPPLIER)

11. INFORMATION / ASSETS

a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information and/or assets on its site or premises?

If Yes, specify the security level of the documents and/or equipment that the supplier will be required to safeguard at their own site or premises using the summary chart.

b) Will the supplier be required to safeguard COMSEC information or assets?

If Yes, specify the security level of COMSEC information or assets that the supplier will be required to safeguard at their own site or premises using the summary chart.

PRODUCTION

c) Will the production (manufacture, repair and/or modification) of PROTECTED and/or CLASSIFIED material and/or equipment occur at the supplier's site or premises?

Using the summary chart, specify the security level of material and/or equipment that the supplier manufactured, repaired and/or modified and will be required to safeguard at their own site or premises.

INFORMATION TECHNOLOGY (IT)

d) Will the supplier be required to use its IT systems to electronically process and/or produce or store PROTECTED and/or CLASSIFIED information and/or data?

If Yes, specify the security level in the summary chart. This block details the information and/or data that will be electronically processed or produced and stored on a computer system. The client department and/or organization will be required to specify the IT security requirements for this procurement in a separate technical document. The supplier must also direct their attention to the following document: Treasury Board of Canada Secretariat - Operational Security Standard: Management of Information Technology Security (MITS).

e) Will there be an electronic link between the supplier’s IT systems and the government department or agency?

If Yes, the supplier must have their IT system(s) approved. The Client Department must also provide the Connectivity Criteria detailing the conditions and the level of access for the electronic link (usually not higher than PROTECTED B level).

SUMMARY CHART

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier’s site(s) or premises.

For users completing the form **online** (via the Internet), the Summary Chart is automatically populated by your responses to previous questions.

PROTECTED	CLASSIFIED	NATO	COMSEC
PROTECTED A	CONFIDENTIAL	NATO RESTRICTED	PROTECTED A
PROTECTED B	SECRET	NATO CONFIDENTIAL	PROTECTED B
PROTECTED C	TOP SECRET	NATO SECRET	PROTECTED C
	TOP SECRET (SIGINT)	COSMIC TOP SECRET	CONFIDENTIAL
			SECRET
			TOP SECRET

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?

If Yes, classify this form by annotating the top and bottom in the area entitled “Security Classification”.

b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?

If Yes, classify this form by annotating the top and bottom in the area entitled “Security Classification” and indicate with attachments (e.g. SECRET with Attachments).

PART D - AUTHORIZATION

13. Organization Project Authority

This block is to be completed and signed by the appropriate project authority within the client department or organization (e.g. the person responsible for this project or the person who has knowledge of the requirement at the client department or organization). This person may on occasion be contacted to clarify information on the form.

14. Organization Security Authority

This block is to be signed by the Departmental Security Officer (DSO) (or delegate) of the department identified in Block 1, or the security official of the prime contractor.

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?

A Security Guide or Security Classification Guide is used in conjunction with the SRCL to identify additional security requirements which do not appear in the SRCL, and/or to offer clarification to specific areas of the SRCL.

16. Procurement Officer

This block is to be signed by the procurement officer acting as the contract or subcontract manager.

17. Contracting Security Authority

This block is to be signed by the Contract Security Official. Where PWGSC is the Contract Security Authority, Canadian and International Industrial Security Directorate (CIISD) will complete this block.

Instructions pour établir la Liste de vérification des exigences relatives à la sécurité (LVERS)

La feuille d'instructions devrait rester jointe au formulaire jusqu'à ce que la case 17 ait été remplie.

GÉNÉRALITÉS - TRAITEMENT DU PRÉSENT FORMULAIRE

Le responsable du projet doit faire remplir ce formulaire.

L'agent de sécurité de l'organisation doit revoir et approuver les exigences de sécurité qui figurent dans le formulaire, en collaboration avec le responsable du projet.

Le responsable de la sécurité des marchés est le responsable chargé de voir à ce que les fournisseurs se conforment aux exigences de sécurité mentionnées dans la LVERS.

Toutes les demandes d'achat ainsi que tous les appels d'offres et les documents contractuels subséquents, y compris les contrats de sous-traitance, qui comprennent des exigences relatives à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS doivent être accompagnés d'une LVERS dûment remplie.

Il importe d'indiquer si les renseignements ou les biens PROTÉGÉS sont de niveau A, B ou C, le cas échéant; cependant, certains types de renseignements peuvent être indiqués par la mention « PROTÉGÉ » seulement. Aucun renseignement relatif à un contrat gouvernemental PROTÉGÉ ou CLASSIFIÉ ne peut être divulgué par les fournisseurs sans l'approbation écrite préalable de la personne dont le nom figure à la case 17 de ce formulaire.

La classification assignée à un stade particulier du processus contractuel ne signifie pas que tout ce qui se rapporte à ce stade doit recevoir la même classification. Chaque article doit être PROTÉGÉ et/ou CLASSIFIÉ selon sa propre nature. Si un fournisseur ne sait pas quel niveau de classification assigner, il doit consulter la personne dont le nom figure à la case 17 de ce formulaire.

PARTIE A - INFORMATION CONTRACTUELLE

Numéro du contrat (au haut du formulaire)

Ce numéro doit être le même que celui utilisé sur la demande d'achat et services et devrait être celui utilisé dans la DDP ou dans le contrat. Il s'agit d'un numéro unique (c.-à-d. que le même numéro ne sera pas attribué à deux besoins distincts). Une nouvelle LVERS doit être utilisée pour chaque nouveau besoin ou demande (p. ex. un nouveau numéro de contrat, une nouvelle LVERS, de nouvelles signatures).

1. Ministère ou organisme gouvernemental d'origine

Inscrire le nom du ministère ou de l'organisme client ou le nom de l'entrepreneur principal pour qui les travaux sont effectués.

2. Direction générale ou Direction

Cette case peut servir à fournir plus de détails quant à la section du ministère ou de l'organisme pour qui les travaux sont effectués.

3. a) Numéro du contrat de sous-traitance

S'il y a lieu, ce numéro correspond au numéro généré par l'entrepreneur principal pour gérer le travail avec son sous-traitant.

b) Nom et adresse du sous-traitant

Indiquer le nom et l'adresse au complet du sous-traitant, s'il y a lieu.

4. Brève description du travail

Donner un bref aperçu du besoin ou du travail à exécuter.

5. a) Le fournisseur aura-t-il accès à des marchandises contrôlées?

La *Loi sur la production de défense* (LPD) définit « marchandises contrôlées » comme désignant certains biens énumérés dans la Liste des marchandises d'exportation contrôlée, un règlement établi en vertu de la *Loi sur les licences d'exportation et d'importation* (LLEI). Les fournisseurs qui examinent, possèdent ou transfèrent des marchandises contrôlées à l'intérieur du Canada doivent s'inscrire à la Direction des marchandises contrôlées ou être exemptés de l'inscription. On trouvera plus d'information à l'adresse www.cgp.gc.ca.

b) Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?

L'entrepreneur et tout sous-traitant doivent être accrédités en vertu du Programme mixte d'agrément Etats-Unis / Canada si le travail comporte l'accès à des données militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques. On trouvera plus d'information à l'adresse www.dlis.dla.mil/jcp/.

6. Indiquer le type d'accès requis

Indiquer la nature du travail à exécuter pour répondre à ce besoin. L'utilisateur doit choisir un des types suivants :

a) Le fournisseur et ses employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS?

Le fournisseur choisit cette option s'il doit avoir accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS pour accomplir le travail requis.

b) Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.

Le fournisseur choisit cette option seulement s'il doit avoir accès régulièrement aux locaux du gouvernement ou à un lieu de travail protégé. Le fournisseur n'aura pas accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS en vertu de cette option.

c) S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit?

Le fournisseur choisit cette option s'il y a nécessité de recourir à un service de messagerie ou de livraison commerciale. Le fournisseur ne sera pas autorisé à garder un colis pendant la nuit. Le colis doit être retourné s'il ne peut pas être livré.

7. Type d'information / Restrictions relatives à la diffusion / Niveau d'information

Indiquer le ou les types d'information auxquels le fournisseur peut devoir avoir accès, énumérer toutes les restrictions possibles relatives à la diffusion, et, s'il y a lieu, indiquer le ou les niveaux d'information. L'utilisateur peut faire plusieurs choix selon la nature du travail à exécuter.

Les ministères doivent soumettre la LVERS à TPSGC lorsque:

- les marchés prévoient l'accès aux renseignements et aux biens de nature PROTÉGÉS et/ou CLASSIFIÉS étrangers ;
- les marchés prévoient aux entrepreneurs étrangers l'accès aux renseignements et aux biens de nature PROTÉGÉS et/ou CLASSIFIÉS canadiens; ou
- les marchés prévoient aux entrepreneurs étrangers ou canadiens l'accès aux renseignements et aux biens de nature PROTÉGÉS et/ou CLASSIFIÉS tels que définis dans les documents intitulés Moyens INFOSEC détermination et Divulgateion de INFOSEC.

a) Indiquer le type d'information auquel le fournisseur devra avoir accès

Renseignements et/ou biens du gouvernement canadien

Si des renseignements et/ou des biens canadiens sont indiqués, le fournisseur aura accès à des renseignements et/ou à des biens PROTÉGÉS et/ou CLASSIFIÉS appartenant au gouvernement canadien.

Renseignements et/ou biens de l'OTAN

Si des renseignements et/ou des biens de l'OTAN sont indiqués, cela signifie que, dans le cadre de ce besoin, le fournisseur aura accès à des renseignements et/ou à des biens PROTÉGÉS et/ou CLASSIFIÉS appartenant à des gouvernements membres de l'OTAN. Les renseignements et/ou les biens de l'OTAN sont élaborés par des pays de l'OTAN ou leur appartiennent et ne doivent être divulgués à aucun pays qui n'est pas un pays membre de l'OTAN. Les personnes qui manient des renseignements et/ou des biens de l'OTAN doivent détenir une autorisation de sécurité de l'OTAN et avoir besoin de savoir.

Les contrats comportant des renseignements CLASSIFIÉS de l'OTAN doivent être attribués par TPSGC. La DSICI de TPSGC est le responsable de la sécurité désigné relativement aux questions de sécurité industrielle au Canada.

Renseignements et/ou biens de gouvernements étrangers

Si des renseignements et/ou des biens de gouvernements étrangers sont indiqués, ce besoin permettra l'accès à des renseignements et/ou à des biens appartenant à un pays autre que le Canada.

b) Restrictions relatives à la diffusion

Si **À ne pas diffuser** est choisi, cela indique que les renseignements et/ou les biens sont **réservés aux Canadiens**. Seuls des fournisseurs canadiens installés au Canada peuvent soumissionner ce genre de besoin. NOTA : Si des renseignements et/ou des biens du gouvernement canadien coexistent avec des renseignements et/ou des biens réservés aux Canadiens, ceux-ci doivent porter la mention **Réservé aux Canadiens**.

Si **Aucune restriction relative à la diffusion** est choisi, cela indique que l'accès aux renseignements et/ou aux biens n'est assujéti à aucune restriction.

Si **Tous les pays de l'OTAN** est choisi, les soumissionnaires doivent appartenir à un pays membre de l'OTAN.

NOTA : Il peut y avoir plus d'une restriction s'appliquant à une demande, selon la nature des travaux à exécuter. Pour ce genre de contrat, un guide de sécurité doit être joint à la LVERS afin de clarifier les restrictions. Ce guide est généralement préparé par le chargé de projet et/ou le responsable de la sécurité de l'organisme.

c) Niveau d'information

À l'aide du tableau ci-dessous, indiquer le niveau approprié d'accès aux renseignements et/ou aux biens que le fournisseur doit avoir pour accomplir les travaux requis.

PROTÉGÉ	CLASSIFIÉ	NATO
PROTÉGÉ A	CONFIDENTIEL	NATO NON CLASSIFIÉ
PROTÉGÉ B	SECRET	NATO DIFFUSION RESTREINTE
PROTÉGÉ C	TRÈS SECRET	NATO CONFIDENTIEL
	TRÈS SECRET (SIGINT)	NATO SECRET
		COSMIC TRÈS SECRET

8. Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS?

Si la réponse est Oui, les membres du personnel du fournisseur qui doivent avoir accès à des renseignements ou à des biens COMSEC doivent participer à une séance d'information COMSEC. Cette séance sera donnée au « détenteur autorisé » des renseignements ou des biens COMSEC. Dans le cas des contrats du type « personnel affecté », cette séance sera donnée par le ministère client. Lorsque le fournisseur doit recevoir et conserver, dans ses locaux, des renseignements ou des biens COMSEC, le responsable de la garde des renseignements ou des biens COMSEC de l'entreprise donnera la séance d'information COMSEC aux membres du personnel qui doivent avoir accès à des renseignements ou à des biens COMSEC.

9. Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

Si la réponse est Oui, le fournisseur doit indiquer le titre abrégé du document, le numéro du document et le niveau de sensibilité. L'accès à des renseignements ou à des biens extrêmement délicats INFOSEC exigera que le fournisseur fasse l'objet d'une vérification Participation, contrôle et influence étrangers (PCIE) effectuée par la DSIC1.

PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Niveau de contrôle de la sécurité du personnel requis

Indiquer le niveau d'autorisation de sécurité que le personnel doit détenir pour avoir accès aux renseignements, aux biens ou au site du client. Selon la nature du travail, il peut y avoir plus d'un niveau de sécurité. Veuillez noter que des cotes de sécurité sont accordées pour l'accès à des sites particuliers, selon des dispositions antérieures prises auprès du Secrétariat du Conseil du Trésor du Canada. La cote de sécurité donnant accès à un site s'applique uniquement aux personnes et n'est liée à aucune autre autorisation de sécurité accordée à des personnes ou à des organismes.

COTE DE FIABILITÉ	CONFIDENTIEL	SECRET
TRÈS SECRET	TRÈS SECRET (SIGINT)	NATO CONFIDENTIEL
NATO SECRET	COSMIC TRÈS SECRET	ACCÈS AUX EMBLEMES

Si plusieurs niveaux d'autorisation de sécurité sont indiqués, un guide de classification de sécurité doit être fourni.

b) Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

Si la réponse est Oui, cela veut dire que certaines tâches ne sont pas PROTÉGÉES et/ou CLASSIFIÉES et peuvent être exécutées à l'extérieur d'un environnement sécurisé par du personnel n'ayant pas d'autorisation de sécurité. Il faut répondre à la question suivante si l'on a recours à du personnel n'ayant pas d'autorisation de sécurité :

Le personnel n'ayant pas d'autorisation de sécurité sera-t-il escorté?

Si la réponse est Non, le personnel n'ayant pas d'autorisation de sécurité ne pourra pas avoir accès à des lieux de travail dont l'accès est réglementé ni à des renseignements et/ou à des biens PROTÉGÉS et/ou CLASSIFIÉS.

Si la réponse est Oui, le personnel n'ayant pas d'autorisation de sécurité devra être escorté par une personne détenant la cote de sécurité requise, pour faire en sorte que le personnel en question n'ait pas accès à des renseignements et/ou à des biens PROTÉGÉS et/ou CLASSIFIÉS sur les lieux de travail.

PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

11. RENSEIGNEMENTS / BIENS :

a) Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

Si la réponse est Oui, préciser, à l'aide du tableau récapitulatif, le niveau de sécurité des documents ou de l'équipement que le fournisseur devra protéger dans ses installations.

b) Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

Si la réponse est Oui, préciser, à l'aide du tableau récapitulatif, le niveau de sécurité des renseignements ou des biens COMSEC que le fournisseur devra protéger dans ses installations.

PRODUCTION

c) Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ?

Préciser, à l'aide du tableau récapitulatif, le niveau de sécurité du matériel que le fournisseur fabriquera, réparera et/ou modifiera et devra protéger dans ses installations.

TECHNOLOGIE DE L'INFORMATION (TI)

d) Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS?

Si la réponse est Oui, préciser le niveau de sécurité à l'aide du tableau récapitulatif. Cette case porte sur les renseignements qui seront traités ou produits électroniquement et stockés dans un système informatique. Le ministère/organisme client devra préciser les exigences en matière de sécurité de la TI relativement à cet achat dans un document technique distinct. Le fournisseur devra également consulter le document suivant : Secrétariat du Conseil du Trésor du Canada – Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI).

e) Y aura-t-il un lien électronique entre les systèmes informatiques du fournisseur et celui du ministère ou de l'agence gouvernementale?

Si la réponse est Oui, le fournisseur doit faire approuver ses systèmes informatiques. Le ministère client doit aussi fournir les critères de connectivité qui décrivent en détail les conditions et le niveau de sécurité relativement au lien électronique (habituellement pas plus haut que le niveau PROTÉGÉ B).

TABLEAU RÉCAPITULATIF

Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

PROTÉGÉ	CLASSIFIÉ	NATO	COMSEC
PROTÉGÉ A	CONFIDENTIEL	NATO DIFFUSION RESTREINTE	PROTÉGÉ A
PROTÉGÉ B	SECRET	NATO CONFIDENTIEL	PROTÉGÉ B
PROTÉGÉ C	TRÈS SECRET	NATO SECRET	PROTÉGÉ C
	TRÈS SECRET (SIGINT)	COSMIC TRÈS SECRET	CONFIDENTIEL
			SECRET
			TRÈS SECRET

12. a) La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

Si la réponse est Oui, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de

sécurité » au haut et au bas du formulaire.

b) La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

Si la réponse est Oui, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

PARTIE D - AUTORISATION

13. Chargé de projet de l'organisme

Cette case doit être remplie et signée par le chargé de projet pertinent (c.-à-d. la personne qui est responsable de ce projet ou qui connaît le besoin au ministère ou à l'organisme client. On peut, à l'occasion, communiquer avec cette personne pour clarifier des renseignements figurant sur le formulaire.

14. Responsable de la sécurité de l'organisme

Cette case doit être signée par l'agent de la sécurité du ministère (ASM) du ministère indiqué à la case 1 ou par son remplaçant ou par le responsable de la sécurité du fournisseur.

15. Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes?

Un Guide de sécurité ou un Guide de classification de sécurité sont utilisés de concert avec la LVERS pour faire part d'exigences supplémentaires en matière de sécurité qui n'apparaissent pas dans la LVERS et/ou pour éclaircir certaines parties de la LVERS.

16. Agent d'approvisionnement

Cette case doit être signée par l'agent des achats qui fait fonction de gestionnaire du contrat ou du contrat de sous-traitance.

17. Autorité contractante en matière de sécurité

Cette case doit être signée par l'agent de la sécurité du marché. Lorsque TPSGC est le responsable de la sécurité du marché, la Direction de la sécurité industrielle canadienne et internationale (DSICI) doit remplir cette case.



ANNEX “D” – EVALUATION CRITERIA

Software Mandatory Requirements

Item	Mandatory Requirement	Compliant (Y/N)	Reference to bidders proposal
M1	The software must be have been verified against the ITIL Software Scheme (ISS) from a licensed software assessor operating under the ITIL intellectual property managed by AXELOS such as Pink Elephant Inc. or Glenfis AG.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
M2	The company manufacturing the software must have a certification curriculum, training and courses on IT Service Management with the proposed software.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
M3	The software must be fully functional in a Microsoft windows environment, with all components installed on-premise, with no additional middleware or infrastructure services to work with: Windows 7, MS Office 2010, Remote Access Entrust PKI, Adobe Reader XI, Entrust 9.3, MS SCCM, MS Active Directory, Windows File/Print server, Microsoft SQL Service 2008/2012, Windows Server 2008/2012, IIS version 7 or 8.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
M4	<p>The software must provide, with no additional programming, the following modules:</p> <p>Incident and problem management functions to initiate, route, track, and manage incidents, create and link different incident types.</p> <p>Request management functions to log, track and report on users’ requests, create and assign tasks and subtasks, manage users and contact information.</p> <p>Asset management to manage and track all hardware and software assets of an organization.</p> <p>Service Catalogue to manage and report on IT services delivered to client organizations.</p> <p>Self-Service for users to automatically open a ticket against given categories.</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No	



	<p>Customizable Reports and Dashboards to provide summary on incidents, problems and assets, in addition to having a database and reporting structure that is cross-functional across all modules.</p> <p>Workflow processes to automate pre-defined tasks, route tickets and manage approvals.</p>		
M5	The software must have documented procedures for backup and restore and documented infrastructure requirements for server, database and network port rules.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
M6	The software must have off the shelf ability to define different user roles to manage permissions and to be able to use Microsoft Active Directory for users and groups.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
M7	The software must provide off the shelf incoming and outgoing email processing, using SMTP gateway, to send email notifications and to receive incoming emails to create and edit tickets.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
M8	The software must have off the shelf configuration settings to meet security requirements outlined in Appendix A 1 st section. Bidders are required to provide relevant information in their response to each requirement.	<input type="checkbox"/> Yes <input type="checkbox"/> No	

Professional Services Mandatory Requirements

Item	Mandatory Requirement	Compliant (Y/N)	Reference to bidders proposal
M9	The bidder's proposed resource(s) must be an ITIL v3 Certified Practitioner	<input type="checkbox"/> Yes <input type="checkbox"/> No	
M10	The bidder's proposed resource(s) must have IT Service Management certification in the software being selected	<input type="checkbox"/> Yes <input type="checkbox"/> No	



M11	The Bidder's proposed resource(s) must demonstrate five (5) projects, within the past five (5) years, installing and configuring the software being selected in for an organization of 1,000 employees or more	<input type="checkbox"/> Yes <input type="checkbox"/> No	
-----	--	---	--

Security Mandatory Requirements

Item	Mandatory Requirement	Compliant (Yes/No)	Reference to Bidder's Proposal
SM1	The Bidder's proposed resource(s) must hold, at a minimum, a valid Government of Canada personnel security clearance at the level of "Secret" at the time of bid closing.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
SM2	Proof of clearance must be supplied by the Bidder with its technical proposal by either providing a copy of the actual certificate or the certificate number and expiry date.	<input type="checkbox"/> Yes <input type="checkbox"/> No	



Software Mandatory Security Requirements

Item	Mandatory Requirements	Compliant (Yes/No)	Reference to Bidder's Proposal
SM3	<p>Access Enforcement</p> <p>a) The software enforces approved authorizations for logical access to information and system resources in accordance with access control policies.</p> <p>b) The software enforces a role-based access control policy over defined subjects and objects and controls access based upon roles and users authorized to assume such roles.</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
SM4	<p>Session Lock</p> <p>(A) The software prevents further access to the system by initiating a session lock after 20 minutes of inactivity or upon receiving a request from a user.</p> <p>(B) The software retains the session lock until the user re-establishes access.</p> <p>(C) The software conceals, via the session lock, information previously visible on the display with a publicly viewable image</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
SM5	<p>Identification and authentication (organizational users) - The software provides a single sign-on capability for all information system accounts and services.</p> <p>The single sign-on is accomplished by ensuring that the software makes use of network credentials via Integrated Login (AD integration).</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
SM6	<p>Application partitioning</p> <p>The software separates user functionality (including user interface services) from information system management functionality.</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No	



SM7	<p>Transmission Confidentiality and Integrity</p> <p>a) The software protects the confidentiality and integrity of transmitted information (Protected B level).</p> <p>b) The software implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission. The cryptography must be compliant with the requirements of control SC-13.</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
SM8	<p>Cryptographic Protection</p> <p>The software implements FIPS-validated cryptography and CSE approved cryptography in accordance with GC legislation and TB policies, directives and standards – see CSEC ITSB-111 Cryptography Algorithms for Protected information</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
SM9	<p>Session Authenticity</p> <p>a) The software protects the authenticity of communications sessions</p> <p>b) The software invalidates session identifiers upon user logout or other session termination.</p> <p>c) The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated.</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
SM10	<p>Fail in known state</p> <p>The software fails to a known-state preserving system state information in failure.</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No	
SM11	<p>Content of Audit Records</p> <p>The software generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity</p>	<input type="checkbox"/> Yes <input type="checkbox"/> No	



	of any individuals or subjects associated with the event.		
SM12	Response to Audit Processing Failures a) The software is able to send alerts in the event of an audit processing failure. b) The software provides a warning to when allocated audit record storage volume reaches a defined percentage of repository maximum audit record storage capacity.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
SM13	Audit Review, Analysis, and Reporting The software provides the capability to centrally review and analyze audit records from multiple components within the system.	<input type="checkbox"/> Yes <input type="checkbox"/> No	
SM14	Time Stamps a) The software uses internal system clocks to generate time stamps for audit records. b) The software records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	<input type="checkbox"/> Yes <input type="checkbox"/> No	
SM15	Security Alerts, Advisories, and Directives The vendor provides software security alerts, advisories, and directives on an ongoing basis.	<input type="checkbox"/> Yes <input type="checkbox"/> No	

Explanatory Notes – Security Requirements

SM3 - Access Enforcement

- a) Access control policies (e.g., identity-based policies, role-based policies, attribute-based policies) and access enforcement mechanisms (e.g.: access control lists, access control matrices, cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, domains) in information systems.
- b) Role-based access control (RBAC) is an access control policy that restricts information system access to authorized users. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on organizational information systems associated with the organization-defined roles.
When users are assigned to the organizational roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user, but are instead acquired through role assignments.

SM4 - Session Lock

- a) and b) Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined.
This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays.
- c) Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.

SM5 - Identification and authentication

Single sign-on enables users to log in once and gain access to multiple information system resources.

SM6 - Application partitioning

Self-explanatory

SM7 - Transmission Confidentiality and Integrity

- a) This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines).
Protecting the confidentiality and integrity of information can be accomplished by logical means (e.g., employing encryption techniques).
- b) Encrypting information for transmission protects information from unauthorized disclosure and modification.
Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems.

SM8 - Cryptographic Protection

If cryptography is required based on the selection of other security controls or policies, organizations document each type of cryptographic use and the type of cryptography required (e.g., protection of Protected B information: CSE-approved cryptography; provision of digital signatures: FIPS-validated cryptography).

SM9 - Session Authenticity

- a) This control addresses communications protection at the session, versus packet level (e.g., sessions in service-oriented architectures providing web-based services) and establishes grounds for confidence at both ends of communications sessions in ongoing identities of other parties and in the validity of information transmitted.
Authenticity protection includes, for example, protecting against man-in-the-middle attacks/session hijacking and the insertion of false information into sessions.
- b) This control curtails the ability of adversaries from capturing and continuing to employ previously valid session IDs
- c) This control curtails the ability of adversaries from reusing previously valid session IDs.
Employing the concept of randomness in the generation of unique session identifiers helps to protect against brute-force attacks to determine future session identifiers.

SM10 - Fail in known state

Failure in a known secure state helps to prevent the loss of confidentiality, integrity, or availability of information in the event of failures of organizational information systems or system components.

Preserving information system state information facilitates system restart and return to the operational mode of organizations with less disruption of mission/business processes.

SM11 - Content of Audit Records

Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked.

Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred).

SM12 - Response to Audit Processing Failures

- a) Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.
- b) Organizations may have multiple audit data storage repositories distributed across multiple information system components, with each repository having different storage volume capacities.

SM13 - Audit Review, Analysis, and Reporting

Automated mechanisms for centralized reviews and analyses include, for example, Security Information Management products.

SM14 - Time Stamps

Self-explanatory

SM15 - Security Alerts, Advisories, and Directives

Self-explanatory



ANNEX “E” - FINANCIAL EVALUATION CRITERIA

Milestones	Deliverables	Description	Deadline	Fixed Price Cost
1	Software (license)	Provide 35 device licenses with one year maintenance and support.	November 30, 2016	
2	Software Installation	Install Software, Assist with Active Directory, SMTP email, integration	November 30, 2016	
3	Configuration of software modules	Configure the following modules; Incident Management and Problem Management; Self-Serve; Asset Management; Customizable reports and Dashboards; Service Catalogue; Workflows and Approvals; provide FIN IT employees with training and training material.	December 31, 2016	
4	Upload current information into new tool.	Assets, employee first/last name, office number, branch and division, phone number, username, title, etc.	December 31, 2016	
5	Information Flow Enforcement	The software enforces approved authorizations for controlling the flow of information within the system and between interconnected systems. The vendor is required to work closely with FIN and SSC IT groups to define specific architectural solutions in support of this requirement.	March 31, 2017	
6	Developing CONOPS and remediating vulnerabilities (if any)found in the Vulnerability Assessment	Develop CONOPS document for IT Security review and assessment at the end of the design phase	March 31, 2017	



7	Vulnerability Scanning	FIN IT Security will scan for application level vulnerabilities in all the software and infrastructure components at the end of the development / integration phase. The vendor is required to analyze the vulnerability scan reports and remediate all legitimate vulnerabilities.	March 31, 2017	
8	Assist with testing and correction of any errors	The vendor will be on-site assisting with correcting vulnerabilities and/or errors found during Vulnerability/UAT testing and provide guidance.	March 31, 2017	
9	Assist and provide full training to FIN-IT employees on the administration of the tool across all modules	Full training manual to be provided by supplier	March 31, 2017	
Total Bid Price				

Optional Pricing for additional licenses:

Deliverables	Description	Fixed Price Cost Per License
Software (license)	Provide additional device licenses with pro-rated maintenance and support.	



BIDDER FORMS

FORM 1 - BID SUBMISSION FORM													
<p>Bidder's full legal name <i>[Note to Bidders: Bidders who are part of a corporate group should take care to identify the correct corporation as the Bidder.]</i></p>													
<p>Authorized Representative of Bidder for evaluation purposes (e.g., clarifications)</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">Name:</td><td></td></tr> <tr><td>Title:</td><td></td></tr> <tr><td>Address:</td><td></td></tr> <tr><td>Telephone #:</td><td></td></tr> <tr><td>Fax #:</td><td></td></tr> <tr><td>Email:</td><td></td></tr> </table>	Name:		Title:		Address:		Telephone #:		Fax #:		Email:	
Name:													
Title:													
Address:													
Telephone #:													
Fax #:													
Email:													
<p>Bidder's Procurement Business Number (PBN) <i>[see the Standard Instructions 2003]</i> <i>[Note to Bidders: Please ensure that the PBN you provide matches the legal name under which you have submitted your bid. If it does not, the Bidder will be determined based on the legal name provided, not based on the PBN, and the Bidder will be required to submit the PBN that matches the legal name of the Bidder.]</i></p>													
<p>Jurisdiction of Contract: Province or Territory in Canada the Bidder wishes to be the legal jurisdiction applicable to any resulting contract (if other than as specified in solicitation)</p>													
<p>Former Public Servants See the Article in Part 2 of the bid solicitation entitled "Former Public Servant" for a definition of "Former Public Servant".</p>	<p>Is the Bidder a FPS in receipt of a pension as defined in the bid solicitation? Yes ____ No ____</p> <p>If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant "</p> <p>Is the Bidder a FPS who received a lump sum payment under the terms of the Work Force Adjustment Directive? Yes ____ No ____</p> <p>If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant "</p>												
<p>Canadian Content Certification As described in the solicitation, bids with at least 80% Canadian content are being given a preference. <i>[For the definition of Canadian goods and services, consult the PWGSC SACC clause A3050T]</i></p>	<p>On behalf of the Bidder, by signing below, I confirm that <i>[check the box that applies]:</i></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 80%;">At least 80 percent of the bid price consists of Canadian goods and services (as defined in the solicitation)</td> <td style="width: 20%;"></td> </tr> <tr> <td>Less than 80 percent of the bid price consists of Canadian goods and services (as defined in the solicitation)</td> <td></td> </tr> </table>	At least 80 percent of the bid price consists of Canadian goods and services (as defined in the solicitation)		Less than 80 percent of the bid price consists of Canadian goods and services (as defined in the solicitation)									
At least 80 percent of the bid price consists of Canadian goods and services (as defined in the solicitation)													
Less than 80 percent of the bid price consists of Canadian goods and services (as defined in the solicitation)													
<p>Licensed Software Maintenance and Support: <i>(Contracting Authority should only insert when supplemental General Conditions 4004 has been inserted in Part 7).</i></p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td style="width: 30%;">Toll-free Telephone Access:</td><td></td></tr> <tr><td>Toll-Free Fax Access:</td><td></td></tr> <tr><td>E-Mail Access:</td><td></td></tr> <tr><td>Website address for web support:</td><td></td></tr> </table>	Toll-free Telephone Access:		Toll-Free Fax Access:		E-Mail Access:		Website address for web support:					
Toll-free Telephone Access:													
Toll-Free Fax Access:													
E-Mail Access:													
Website address for web support:													



FORM 1 - BID SUBMISSION FORM

Security Clearance Level of Bidder

[include both the level and the date it was granted]

[Note to Bidders: Please ensure that the security clearance matches the legal name of the Bidder. If it does not, the security clearance is not valid for the Bidder.]

On behalf of the Bidder, by signing below, I confirm that I have read the entire bid solicitation including the documents incorporated by reference into the bid solicitation and I certify that:

1. The Bidder considers itself and its products able to meet all the mandatory requirements described in the bid solicitation;
2. This bid is valid for the period requested in the bid solicitation;
3. All the information provided in the bid is complete, true and accurate; and
4. If the Bidder is awarded a contract, it will accept all the terms and conditions set out in the resulting contract clauses included in the bid solicitation.

Signature of Authorized Representative of Bidder



(Delete if N/A)

Form 2 Substantiation of Technical Compliance Form		
Article of Statement of Work that requires substantiation by the Bidder	Bidder Substantiation	Reference to additional Substantiating Materials included in Bid



(Delete if N/A)

**Form 3
OEM Certification Form**

This confirms that the original equipment manufacturer (OEM) identified below has authorized the Bidder named below to provide and maintain its products under any contract resulting from the bid solicitation identified below.

Name of OEM _____

Signature of authorized signatory of OEM _____

Print Name of authorized signatory of OEM _____

Print Title of authorized signatory of OEM _____

Address for authorized signatory of OEM _____

Telephone no. for authorized signatory of OEM _____

Fax no. for authorized signatory of OEM _____

Date signed _____

Solicitation Number _____

Name of Bidder _____



(Delete if N/A)

Form 4 Software Publisher Certification Form (to be used where the Bidder itself is the Software Publisher)	
<p>The Bidder certifies that it is the software publisher of all the following software products and that it has all the rights necessary to license them (and any non-proprietary sub-components incorporated into the software) on a royalty-free basis to Canada pursuant to the terms set out in the resulting contract:</p>	
<hr/>	
<hr/>	
<hr/>	
<hr/>	
<i>[Bidders should add or remove lines as needed]</i>	



(Delete if N/A)

Form 5
Software Publisher Authorization Form
(to be used where the Bidder is not the Software Publisher)

This confirms that the software publisher identified below has authorized the Bidder named below to license its proprietary software products under the contract resulting from the bid solicitation identified below. The software publisher acknowledges that no shrink-wrap or click-wrap or other terms and conditions will apply, and that the contract resulting from the bid solicitation (as amended from time to time by its parties) will represent the entire agreement, including with respect to the license of the software products of the software publisher listed below. The software publisher further acknowledges that, if the method of delivery (such as download) requires a user to "click through" or otherwise acknowledge the application of terms and conditions not included in the bid solicitation, those terms and conditions do not apply to Canada's use of the software products of the software publisher listed below, despite the user clicking "I accept" or signalling in any other way agreement with the additional terms and conditions.

This authorization applies to the following software products:

[Bidders should add or remove lines as needed]

Name of Software Publisher (SP) _____

Signature of authorized signatory of SP _____

Print Name of authorized signatory of SP _____

Print Title of authorized signatory of SP _____

Address for authorized signatory of SP _____

Telephone no. for authorized signatory of SP _____

Fax no. for authorized signatory of SP _____

Date signed _____

Solicitation Number _____

Name of Bidder _____